Cb Protection v8.0.0

Release Note: Enhanced Management of Unidesk Files

Cb Protection 8.0.0
Document Updated: January 2018

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: http://www.carbonblack.com

Copyright © 2004-2018 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Carbon Black is a trademark of Carbon Black, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

Introduction

A Unidesk administrator can create and deploy read-only Unidesk layers, virtual disks that contain applications approved for use in their environment as well as a bootable Windows image. There is also a writeable layer on an endpoint using Unidesk, not deployed by Unidesk but part of the logical structure on the endpoint.

If you deployed the applications in the read-only layers, you likely have already decided that they are safe and appropriate for your environment. If you are using Cb Protection to manage endpoints in a Unidesk environment, you might want to approve the "interesting files" in the read-only Unidesk layers so that users of these layers do not need to request approval for each file. This also allows you to concentrate on tracking the file activity on the write layer.

Automatic local approval of Unidesk read-only files is now supported in Cb Protection.

How Cb Protection Handles Unidesk Files

- **Always Ignore Hidden Volumes:** Unidesk presents its source layers on a system as numerous storage volumes, but only one is mapped as the C: drive. To reduce the amount of file analysis work and eliminate unnecessary cataloging of files, hidden (unmapped) Unidesk volumes and their files are ignored by the agent. This is always true – no configuration setting is necessary.
- **Optional Automatic Approval of Mapped Read-Only Files:** If an optional configuration property is enabled as described below, when a file in the mapped read-only layer is discovered, it is added to the Cb Protection inventory and automatically approved. File discovery (and with this option, approval) in a read-only layer is not automatic; it occurs when the file is executed or a cache consistency check is run.
- **Optionally Ignore File Changes that Occur when Agent is not Running:** By default, Cb Protection uses USN journaling to trigger a cache consistency check when file changes occur when the agent is not running. This can be disabled for better performance with Unidesk.
- **Normal Tracking of Files in the Unidesk Write Layer:** Files in the Unidesk write layer are inventoried and analyzed the same as files on non-Unidesk systems. This includes files provided in the read-only layer but modified so that they must be saved in the write layer.

Note: Modifications to the read-only layer done offline and then returned to the endpoint are not detected until the modified file is executed (or a cache consistency check is run). Also, if a file from the read-only layer is modified and saved to the write layer, then removed from the write layer, the inventory may still reflect the modified version that is no longer there. See Unidesk Layer Changes and File Inventory Accuracy on page 7.

System requirements

To use the Unidesk-Cb Protection integration, systems must meet the following requirements:

- Unidesk 2.9.6 or higher
- Cb Protection Server 8.0.0
- Cb Protection Agent 8.0.0

Note: You can also integrate Unidesk with Bit9 Platform 7.2.3 Patch 5 and later.

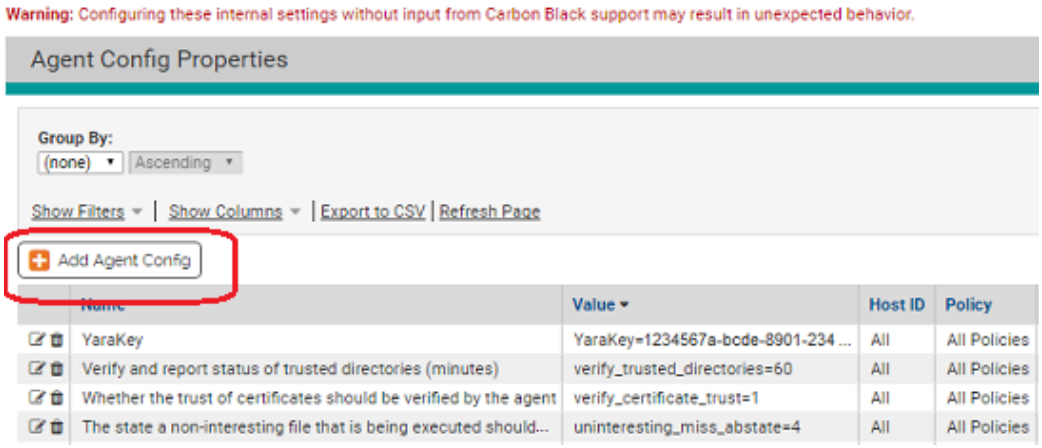
Automatic Approval of Files on Read-only Volumes

The following procedure enables automatic local approval of files on the mapped read-only layers of a Unidesk endpoint as they are discovered by the Cb Protection Agent. Automatic local approval will save you the time and effort required to do individual approvals as they are requested by each user. Keep the following in mind before enabling this feature:

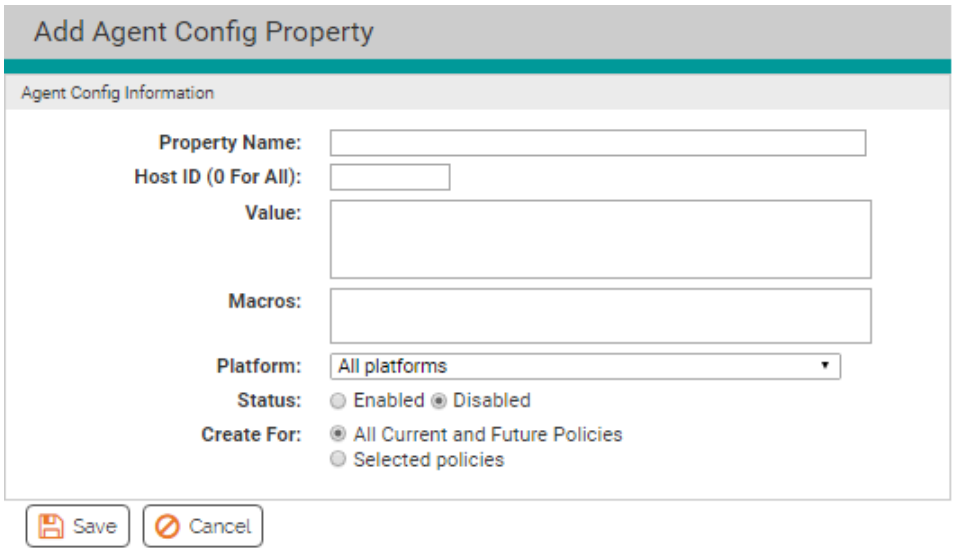
- Be certain that you want to allow approval and execution of *any file* on the read-only layers before you enable this feature.
- Although these files will be approved, the Cb Protection Agent will still perform an analysis on a file the first time it is executed, so you will still see a performance impact in this case. Subsequent executions of the same file will not be impacted.

To enable automatic approval of files found on Unidesk read-only volumes:

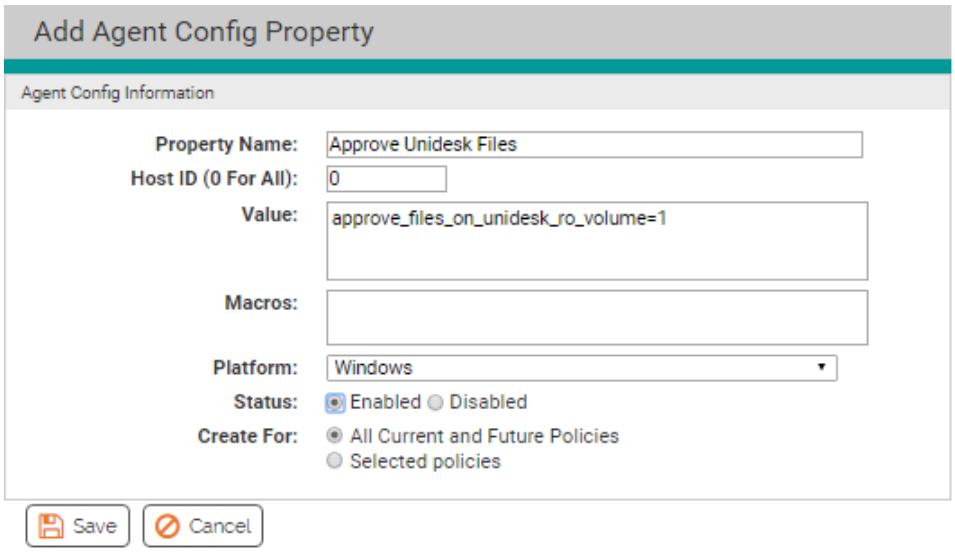
1. Log in to the Cb Protection Server using an account with administrator privileges.
2. Go to the Agent Config Properties page. This is not available through the user interface but is reached by entering the following URL:
   https://<*servernameandpath*>/agent_config.php



3. On the Agent Config Properties page, click **Add Agent Config**. This opens the Add Agent Config Property page.



4. Enter the information for the fields on this page:
   - **Property Name:** `Approve Unidesk Files`
     This can be any name you choose, but for ease of troubleshooting, this standard name is recommended.
   - **Host ID:** Enter zero (0) if you want this property to affect all agents or to agents you specify by policy.
     Note: If you want to specify individual computers for which this setting will be effective, you can enter specific computer IDs, which can be seen in the URL on the Computer Details page for each computer. However, if you want to limit the endpoints on which this setting will be effective, putting all the target endpoints in one policy may be a better choice.
   - **Value:** This ***must*** be the following string:
     `approve_files_on_unidesk_ro_volume=1`
   - **Macros:** You can leave this blank.
   - **Platform:** Unidesk is a Windows application, so you can choose `Windows` here.
   - **Status:** Click the `Enabled` radio button.
   - **Create for:** If you want this to apply to all agent-managed computers, choose **All Current and Future Policies**. If you want to limit this setting to computers in certain policies, click **Selected Policies** and then specify the policies.
5. When you have finished entering the settings for this property, click **Save**.



All files discovered in the Unidesk read-only layer (because they were executed or a cache consistency check was run) will now be automatically locally approved.

You can disable automatic local approval of Unidesk read-only layer files at any time. This will not remove local approval from file instances already approved by this method, but it will prevent local approval of newly discovered instances of files on Unidesk read-only layers.

To disable automatic local approval of Unidesk read-only layer files:

1. Go to the Agent Config Properties page. https://*<servernameandpath>*/agent_config.php
2. On the Agent Config Properties page, double-click the View Details (pencil and box) icon next to the Approve Unidesk Files configuration. This opens the Edit Agent Config Property page.
3. On the Edit Agent Config Property page, click the the **Disabled** radio button and then click **Save**.

Note: If you are certain that you will not want to re-enable this property, you can delete it on the Agent Config Properties page instead of turning it off.

Ignore USN Journal Changes

By default, Cb Protection uses the Windows' NTFS file system to discover files modified when the agent is not running. The agent uses the NTFS USN Journal to gather a list of modified files so that the agent doesn't need to wait until execution time for the files to be seen. This involves running a cache consistency check whenever the USN Journal reports file changes.

Important: Although this feature has obvious plusses, it can cause performance problems in the Unidesk environment, leading to unacceptably high CPU usage. New volumes appearing that the agent did not see before count as a trigger to do the rescan. Because of this, Carbon Black recommends that automatic cache consistency checks triggered by changes reported in the USN Journal be disabled using a special configuration property

To disable automatic cache consistency checks for file changes when agents are not running:

1. Log in to the Cb Protection Server using an account with administrator privileges.
2. Go to the Agent Config Properties page by entering the following URL:
   https://*<servernameandpath>*/agent_config.php
3. On the Agent Config Properties page, click **Add Agent Config**. This opens the Add Agent Config Property page.
4. Enter the information for the fields on this page:
   - **Property Name:** `Disable CC3 on USN Journal Reported Changes`
     This can be any name you choose, but for ease of troubleshooting, this standard name is recommended.
   - **Host ID:** Enter zero (0) if you want this property to affect all agents or to agents you specify by policy.
     Note: If you want to specify individual computers for which this setting will be effective, you can enter specific computer IDs, which can be seen in the URL on the Computer Details page for each computer. However, if you want to limit the endpoints on which this setting will be effective, putting all the target endpoints in one policy may be a better choice.
   - **Value:** This ***must*** be the following string:
     `usn_journal_flags=0`
   - **Macros:** You can leave this blank.
   - **Platform:** Unidesk is a Windows application, so you can choose `Windows` here.
   - **Status:** Click the `Enabled` radio button.
   - **Create for:** If you want this to apply to all agent-managed computers, choose **All Current and Future Policies**. If you want to limit this setting to computers in certain policies, click **Selected Policies** and then specify the policies.
5. When you have finished entering the settings for this property, click **Save**.

Unidesk Approval Events and Alerts

A new event subtype, *File approved (Unidesk),* appears when a file is approved because of the automatic setting for Unidesk read-only layer approvals.

If you choose, you can create an Alert to notify you whenever a file is approved in this way. The alert can also be configured to notify you only when a certain threshold number of files receive Unidesk-based approval, or when only when files on computers in certain policies are approved in this way. Note, however, that this could produce a very large volume of alerts, reducing their usefulness. Consider this before implementing any alert.

You can also use the Unidesk event to trigger actions through Event Rules.

Unidesk Layer Changes and File Inventory Accuracy

Because Unidesk layers may be added and removed from an endpoint, the Cb Protection file inventory for Unidesk systems can be inaccurate to varying degrees. This has the following effects when a read-only layer is removed, changed, and then restored on the endpoint:

- If files are added to the layer, the new files will not be discovered until they are executed or a full cache consistency check is run.
- If files are deleted from the layer, they may stay in the inventory until a full cache consistency check is run. This is also true of all the files in a layer that has been removed and not yet restored on the endpoint.
- If a file in the layer is modified, it may still be in the inventory but have the wrong hash and file information until a full cache consistency check is run. Among the side effects of this case can be:
    - If a file was locally approved because it was on a Unidesk read-only layer, and if a file with the same name but a different hash appears on a new Unidesk layer, the new (but actually different) file might retain the approval from the original file. This can be true for both new read-only layers and changed files on the writable layer.
    - If a file in a Unidesk layer that was not an installer is replaced by a file with the same name, and the new file *is* an installer, the Cb Protection Agent will not recognize this change, and the file will not be "promoted" so that it can run as an installer.
    - Other file information, such as publisher and certificate, might be incorrect.

If you want to maintain the most accurate possible inventory of files on endpoints running Unidesk, consider periodically running a full cache consistency check (CC3) on each endpoint. Because a full cache consistency check can be time consuming, running it during non-critical periods is recommended. You may want to do this whenever you make major changes to a Unidesk layer or on a regular schedule. On the other hand, if you are not concerned about closely tracking the read-only layer, you might not need to run these checks.

Contacting Support

For your convenience, support for Cb Protection is available through several channels:

Technical Support Contact Options
Web: User eXchange
E-mail: support@carbonblack.com
Phone: 877.248.9098
Fax: 617.393.7499

Reporting Problems

When you contact support, please provide the following information to your representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name and version number
Hardware configuration	Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page of most documents and after the Copyrights and Notices section of longer manuals.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement