Netwrix Auditor Add-on for ArcSight

Quick-Start Guide

Version: 9.9
11/14/2019

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. About This Document

This guide is intended for the first-time users of Netwrix Auditor Integration API add-ons. It can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Define add-on parameters
- Execute the add-on
- Review results

NOTE: The add-on works only in combination with Netwrix Auditor so this guide covers a basic procedure for running the add-on and assumes that you have Netwrix Auditor installed and configured in your environment. For installation scenarios, data collection options, as well as detailed information on Integration API, refer to:

- Netwrix Auditor Online Help Center
- Netwrix Auditor Installation and Configuration Guide
- Netwrix Auditor Integration API Guide

1.1. Netwrix Auditor Features and Benefits

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Active Directory Federation Services, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, Nutanix Files, network devices, SharePoint, Oracle Database, SQL Server, VMware, Windows Server, and User Activity. Empowered with a RESTful API, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

Major benefits:

- Detect insider threats—on premises and in the cloud
- Pass compliance audits with less effort and expense
- Increase productivity of IT security and operations teams

To learn how Netwrix Auditor can help your achieve your specific business objectives, refer to Netwrix Auditor Best Practices Guide.

2. Netwrix Auditor Add-on for ArcSight

Netwrix Auditor helps you extend auditing possibilities and get most from your ArcSight investment. The Netwrix Auditor Add-on for ArcSight works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by ArcSight.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to ArcSight. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into native ArcSight CEF format. Each exported event contains the user account, action, time, and other details.
3. The add-on uploads audit trails to ArcSight Logger making it immediately ready for review and analysis. ArcSight SmartConnector configured as Syslog Daemon is supported as well.

For more information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API, refer to Netwrix Auditor Integration API Overview.

2.1. Compatibility Notice

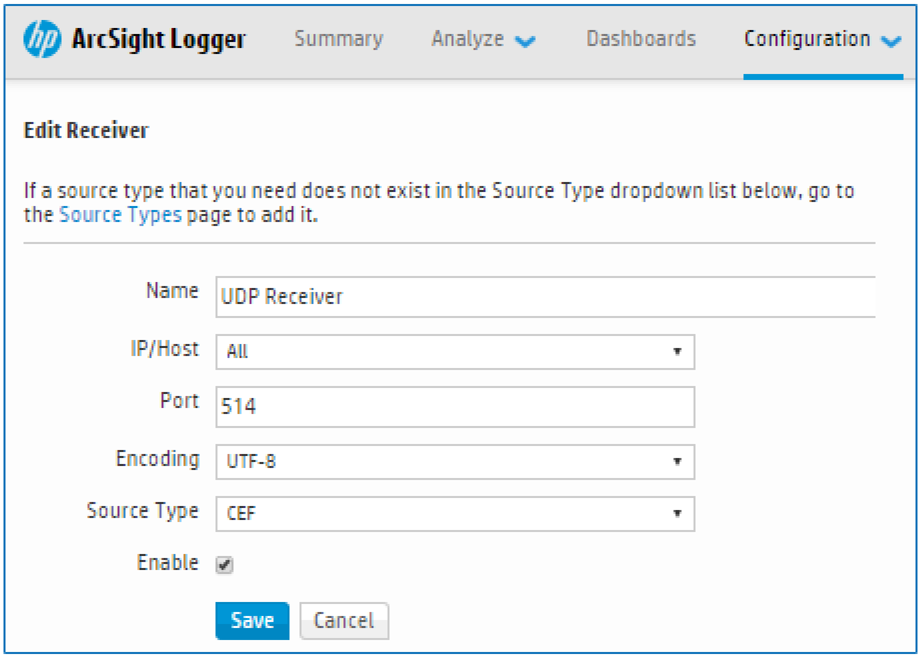
Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store. For more information about schema updates, refer to Netwrix Auditor Integration API.

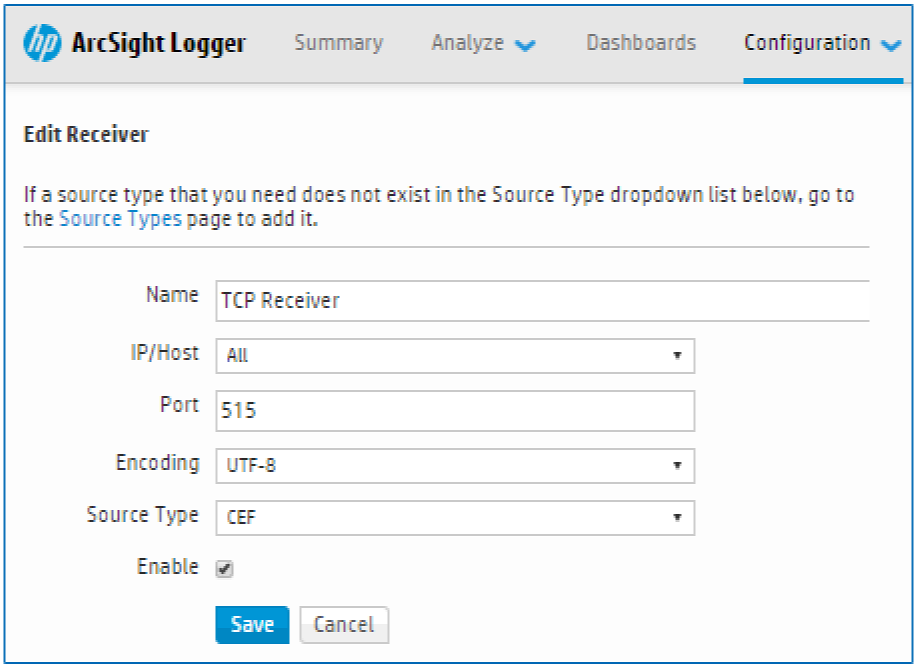
The add-on was renamed due to HPE acquisition by Micro Focus. The former add-on name was Netwrix Auditor Add-on for HPE ArcSight. This name may still be present in the add-on files and documentation. ArcSight trademarks and registered trademarks are property of their respective owners.

3. Use the Add-On

3.1. Prerequisites

Before running Netwrix Auditor Add-on for ArcSight, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Netwrix Auditor Server side	• The Audit Database settings are configured in Netwrix Auditor Server. • The TCP 9699 port (default Netwrix Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the **Global reviewer** role in Netwrix Auditor or is a member of the **Netwrix Auditor Client Users** group. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.
On the ArcSight side	• The UDP Receiver is enabled and is configured to receive CEF as source and use the default port 514. To check receiver settings or add a new receiver, start the ArcSight Logger web interface and navigate to **Configuration** → **Receivers**.  ArcSight Logger Summary Analyze Dashboards Configuration Save Cancel Edit Receiver If a source type that you need does not exist in the Source Type dropdown list below, go to the Source Types page to add it. Name: UDP Receiver IP/Host: All Port: 514 Encoding: UTF-8 Source Type: CEF Enable: ☑

On...	Ensure that...
	NOTE: You can configure TCP Receiver and switch to TCP protocol and port 515.  ArcSight Logger Summary Analyze Dashboards Configuration Save Cancel Edit Receiver If a source type that you need does not exist in the Source Type dropdown list below, go to the Source Types page to add it. Name: TCP Receiver IP/Host: All Port: 515 Encoding: UTF-8 Source Type: CEF Enable: ☑ • The user running the script must have sufficient permissions to supply data to ArcSight.
The computer where the script will be executed	• Execution policy for powershell scripts is set to *"Unrestricted"*. Run **Windows PowerShell** as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the **write** permission on the script folder—the add-on creates a special .bin file with the last exported event.

3.2. Define Parameters for Add-On

Before running or scheduling the add-on, you must define connection details: Netwrix Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See Choose Appropriate Execution Scenario for more information.

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters—the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Parameter or switch	Default value	Description
TCP	—	By default, UDP protocol is used. Specify the switch during the add-on execution if you want to use TCP protocol for transferring data. Via UDP, events will be sent one by one, via TCP—in a batch.
ArcSightHost	—	Provide a name of the computer where ArcSight resides (e.g., 172.28.6.18, ArcSightSRV, ArcSightSRV.enterprise.local). **NOTE:** This is a mandatory parameter. Unless specified, the add-on assumes that the default port 514 is used for UDP and 515 for TCP. To specify a non-default port, provide a server name followed by the port number (e.g., ArcSightSRV.enterprise.local:9998).
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Netwrix Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Netwrix Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Netwrix Auditor Server, specify the account name in the DOMAIN\username format. **NOTE:** The account must be assigned the **Global reviewer** role in Netwrix Auditor or be a member of the **Netwrix Auditor Client Users** group on the computer hosting Netwrix Auditor Server.
NetwrixAuditorPassword	Current user	Unless specified, the script runs with the current

Parameter or switch	Default value	Description
	credentials	user credentials. Provide a different password if necessary.

3.3. Choose Appropriate Execution Scenario

Netwrix Auditor Add-on for ArcSight runs on any computer in your environment. For example, you can run the add-on on the computer where Netwrix Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters.See Netwrix Auditor Add-on for ArcSight for more information.

Netwrix suggests the following execution scenarios:

Scenario	Example

The add-on runs on the Netwrix Auditor Server with the current user credentials. Data is written a remote ArcSight through UDP protocol.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_`
	`ArcSight.ps1 -ArcSightHost 172.28.6.18`

The add-on runs on the Netwrix Auditor Server with the current user credentials. Data is written a remote ArcSight through TCP protocol.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_`
	`ArcSight.ps1 -TCP`
	`-ArcSightHost 172.28.6.18`

The add-on runs on the Netwrix Auditor Server with the explicitly specified user credentials. Data is written a remote ArcSight with a non-default UDP port.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_`
	`ArcSight.ps1 -ArcSightHost 172.28.6.18:9999`
	`-NetwrixAuditorUserName enterprise\NAuser -`
	`NetwrixAuditorPassword NetwrixIsCool`

The add-on runs on a remote computer with the current user credentials. Data is retrieved from a remote Netwrix Auditor repository and written to a remote ArcSight.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_`
	`ArcSight.ps1 -ArcSightHost 172.28.6.24 -`
	`NetwrixAuditorHost 172.28.6.15`

The add-on runs on a remote computer. Data is retrieved from a remote Netwrix Auditor repository with the explicitly specified user credentials and written to a remote ArcSight.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_`
	`ArcSight.ps1 -ArcSightHost 172.28.6.24 -`
	`NetwrixAuditorHost 172.28.6.15`
	`-NetwrixAuditorUserName enterprise\NAuser`
	`-NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Netwrix Auditor data and ArcSight and use it for running the script.

3.4. Run the Add-On with PowerShell

To run the script with PowerShell

1. On computer where you want to execute the add-on, start **Windows PowerShell**.

2. Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

3. Add script parameters. The console will look similar to the following:

   ```
   Windows PowerShell
   Copyright (C) 2014 Microsoft Corporation. All rights reserved.
   PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ArcSight.ps1 -
   ArcSightHost 172.28.6.24 -NetwrixAuditorHost 172.28.6.15
   ```

   NOTE: If the script path contains spaces (e.g., `C:\Netwrix Add-ons\`), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., `& "C:\Netwrix Add-ons\"`).

4. Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix AuditorAudit Database execution may take a while. Ensure the script execution completed successfully. As a result, data will be exported to ArcSight. Note that events exceeding 4000 symbols are trimmed.

Every time you run the script, Netwrix Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records.

3.5. Automate Add-On Execution

To ensure you feed the most recent data to ArcSight, Netwrix recommends scheduling a daily task for running the add-on.

To create a scheduled task

1. On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

2. Select **Create Task**.

3. On the **General** tab, specify a task name, e.g., Netwrix Auditor Add-on for ArcSight. Make sure the account that runs the task has all necessary rights and permissions.

4. On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Netwrix Auditor and transferred to ArcSight Logger. Netwrix recommends scheduling a daily task.

5. On the **Actions** tab, click **New** and specify action details. Review the following for additional

information:

Option	Value
Action	Set to *"Start a program"*.
Program/script	Input *"Powershell.exe"*.
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ArcSight.ps1" -ArcSightHost 172.28.6.24 -NetwrixAuditorHost 172.28.6.15`

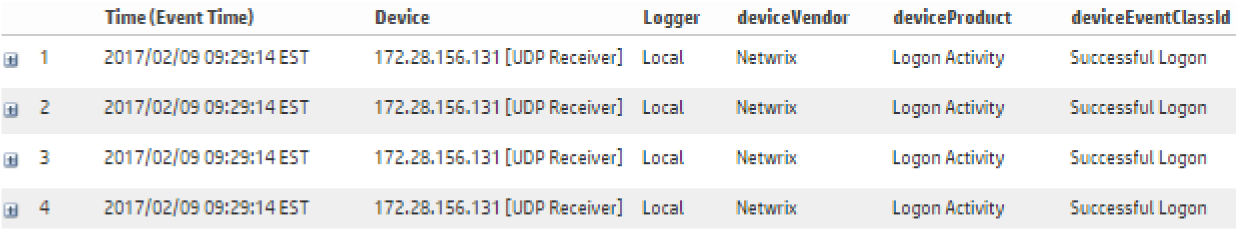
6. Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

3.6. See Results

1. For example, log on to your **ArcSight Logger** web interface.
2. On the **Summary** page, select the **Event Summary by Receiver** diagram and click the **UDP Receiver** segment (Activity Records are imported through UDP Receiver). Select **TCP Receiver** if you specified TCP protocol for trasferring data.
3. On the **Analyze** page that opens, review the search field. Ensure your computer is listed as Receiver (e.g., "172.28.156.131 [UDP Receiver]"). If you imported Activity Records from more than one Netwrix Auditor Server, add all of them in the search field.

   NOTE: You might want to modify time range and the fields shown.
4. Review imported Activity Records.



		Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceEventClassId
⊞	1	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon
⊞	2	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon
⊞	3	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon
⊞	4	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon

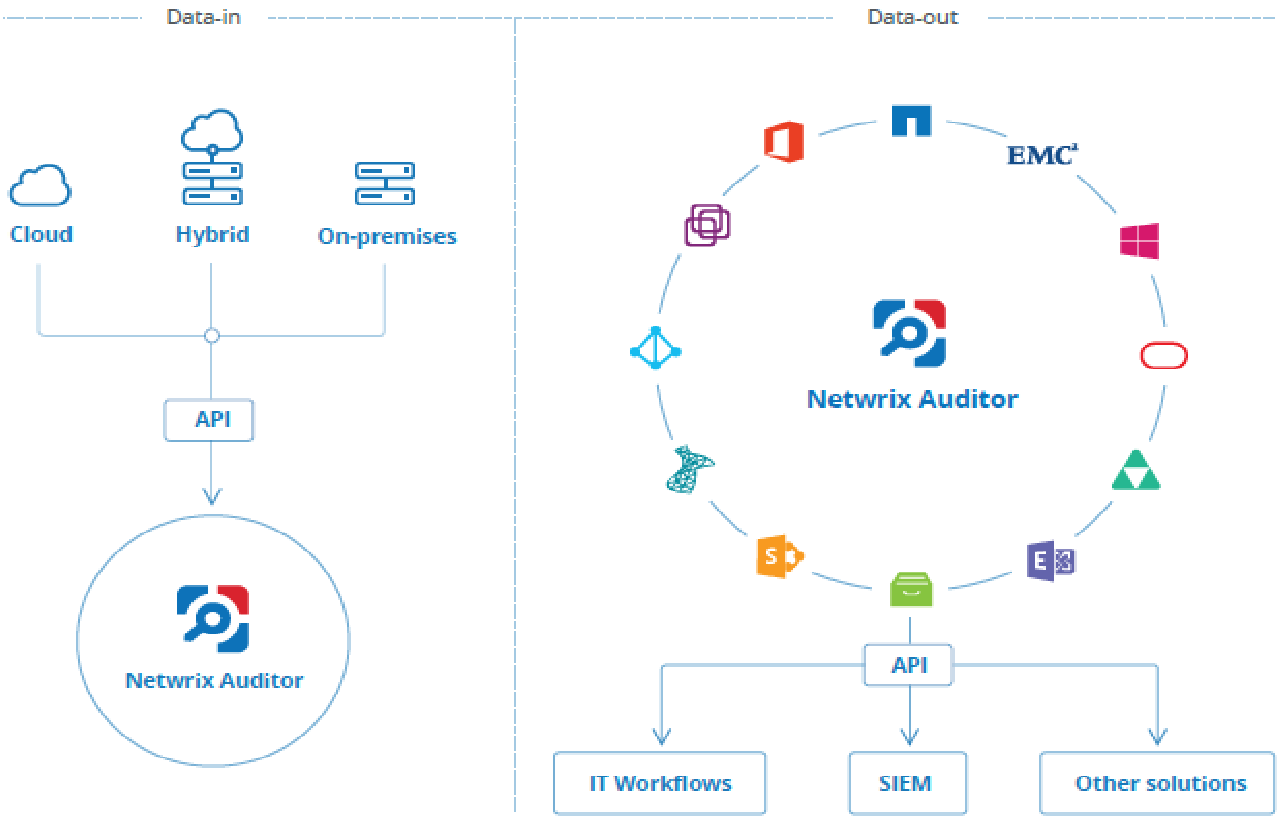
4. Netwrix Auditor Integration API Overview

Netwrix Auditor Add-on for ArcSight leverages Netwrix Auditor Integration API. Although you can always use the add-on as is, but Netwrix encourages customers to create their own integration add-ons. The add-ons created based on Netwrix Auditor Integration API capabilities are easily tailored to your specific environment and business requirements.

Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

The Netwrix Auditor Integration API provides access to audit data collected by Netwrix Auditor through REST API endpoints. According to the RESTful model, each operation is associated with a URL. Integration API provides the following capabilities:

- **Data in**: Solidify security and meet regulatory compliance standards by enabling visibility into what is going on in any third-party application.
- **Data out**: Further automate your business processes, IT security and operations workflows by enriching third-party solutions with actionable audit data.



Netwrix Auditor Integration API operates with XML- and JSON-formatted Activity Records—minimal chunks of audit data containing information on *who* changed *what*, *when* and *where* this change was made. XML format is set as default.

With Integration API you can write Activity Records to the SQL Server-based Audit Database and access audit data from remote computers. Also, Netwrix prepares add-ons—sample scripts—to help you integrate your SIEM solutions with Netwrix Auditor.

Netwrix Auditor Integration API Service is responsible for processing API requests. This component is installed along with Netwrix Auditor Server and is enabled automatically. By default, Netwrix Auditor Integration API works over HTTPS protocol using an automatically generated certificate. Default communication port is **9699**.

Netwrix does not limit you with applications that can be used with Integration API. You can write RESTful requests using any tool or application you prefer—cURL, Telerik Fiddler, various Google Chrome or Mozilla FireFox plug-ins, etc.

See Netwrix Auditor Integration API Guide for more information.