



# Tripwire State Analyzer Report Catalog

Tripwire® State Analyzer automates change alerts. It works in tandem with Tripwire Enterprise and Tripwire IP360™ to provide smart alerting and automation in critical security areas that are not manageable by traditional system state monitoring approaches.

Originally developed for customers with high security requirements in the electric generation and transmission utilities industry, its high adoption rate now spans multiple industries that face similar monitoring challenges.

Tripwire State Analyzer is scalable, flexible, and easy to maintain. This document highlights available reports.

## Users and Passwords

In the solution for local users, multiple aspects of user accounts are reported on.

The solution has built-in options which allow for:

- » Addition of custom fields
- » Option of readable output, or CSV output
- » Alerting on password over allowed age limit
- » Alerting on passwords nearing allowed age limit

## Evidence Reporting

### Local Users and Passwords

Report by asset

Reference (Windows Server)

Local Users Extended - Documentation [Windows Server]

#### Local Users

Version : 8/27/14 2:35 PM  
Type : Modified

#### Content

Reporting includes  
Justification and  
password age analysis

Local User: Administrator  
Status: Enabled  
Password Max Age Allowed: 365  
Password Age Actual: 288  
Last Login Time: 8/27/2014 2:29:08 PM  
Full Name: No Real Name  
Justification: Built-in Administrator Account  
Manager/Responsible Team: No Manager

### Local Users and Passwords

ht-linux.heldtech.com (Linux Server)

Local Users Extended - Documentation [Linux Server]

#### Local Users

Version :

Type :  
Content

Example user account  
not allowlisted

```
*****  
** UNAUTHORIZED LOCAL USER FOUND **  
*****  
Local User: root  
Status: Enabled  
Password Max Age Allowed: N/A  
Password Age Actual: 1141  
Last Login Time: Aug 17 12:37 -
```

## Security Alerting

### Drilldown - Detailed test results

Ensure No Unauthorized Local Users or Expired Passwords Exist

Node: ht-tripwire.heldtech.com (Linux Server)

Overall result: Failed @ 10/8/13 12:39 PM

Element: Unauthorized Local Users

**Result**

Failed

**Time**

10/8/13 12:39 PM

**Actual**

Unauthorized Users=\_\_\_\_\_

\*\*\*\*\*

**\*\* UNAUTHORIZED LOCAL USER FOUND \*\***

\*\*\*\*\*

Local User: tripwire

Status: Enabled

Password Max Age Allowed: N/A

Password Age Actual: 537

Last Login Time: \_\_\_\_\_

An account found that needs to be allowlisted or removed from the system

Systems with new unauthorized users or state passwords have change indicators from green to red. This example shows a detailed report of just the exceptions that a System Administrator should attend to.

### Support and Requirements

This solution is supported on:

- » Windows
- » RHEL

## Ports

Reports are generated to support two use cases: evidence reporting and alerting for daily maintenance of compliance. Report generation is automated once the solution is fully implemented, and allows for scanning as often as is desired.

## Evidence Reporting

**Report by Asset**

**Justification for each allowed port**

**Ports lacking justification called out**

```
Network Ports - Documentation [Windows]
W2K8_SIEMENS_HMI (Windows Server)
Network Ports - Documentation [Windows] (Command Output Capture Rule)

ports
-----
Version :      5/16/13 12:59 PM
Type :        Modified
Content

Protocol: TCP
Port Number: 80
Process name: System
Process Description: Hypertext Transfer Protocol
Justification: Default port for web server
Documentation: Required by web servers

Protocol: TCP
Port Number: 135
Process name: svchost.exe
Process Description: Microsoft Windows Service Host Process / Generic Host Process for Win32 Services
Justification: Used by Microsoft Windows for administering dynamically linked library files (DLL files) and other supplementary support applications
Documentation: See http://www.processlibrary.com/directory/files/svchost/24778/

*****
** UNAUTHORIZED PORT FOUND **
*****
Protocol: TCP
Port Number: 443
Process name: java.exe

Protocol: TCP
Port Number: 445
Process name: System
Process Description: Microsoft Windows Server Message Block
```

The solution has built-in options which allow for:

- » Ephemeral ports
- » Port ranges
- » TCP and UDP
- » Digest data from nmap or IP360
- » Matching ports to process
- » Addition of custom fields to reports

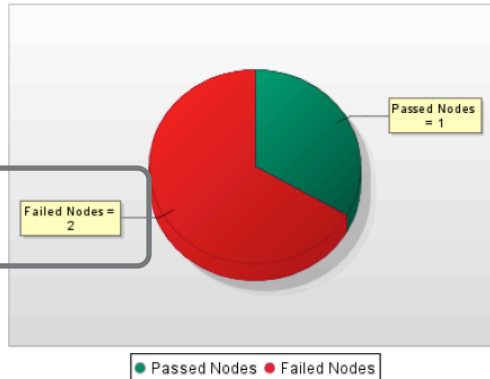
## Support and Requirements

This solution is supported on:

- » Agent-based, internal scanning:
  - Windows
  - RHEL
  - AIX
  - Solaris
- » Agentless, external scanning for an IP device

## Compliance Alerting

### Unauthorized Ports on Windows



Immediate indication if an unexpected port is detected

#### Ensure No Unauthorized Listening Ports Exist

The Responsible Entity shall enable only those ports and services required for normal and emergency operations

Node	Passed Tests	Failed Tests	Percent Compliant
JTI-NERC-XP	1	0	100%
Server2008r2Ent	0	1	0%
W2K_SIEMENS_HMI	0	1	0%

Drill-down on an asset to show details of unexpected ports

### Detailed Test Results Template

#### Ensure No Unauthorized Listening Ports Exist

The Responsible Entity shall enable only those ports and services

Node: W2K\_SIEMENS\_HMI (Windows Server)

Overall result: Failed @ 5/20/13 7:17 PM

Element: Unauthorized Network Ports

#### Result

Failed

#### Time

12/18/14 2:55 PM

#### Actual

Unauthorized ports=

```
*****  
** UNAUTHORIZED PORT FOUND **  
*****
```

Protocol: TCP  
Port Number: 17500  
Process name: Dropbox.exe

```
*****  
** UNAUTHORIZED PORT FOUND **  
*****
```

Protocol: UDP  
Port Number: 17500  
Process name: Dropbox.exe

Return to a compliant state by closing or justifying the port

## Services

Once the user has supplied information about normal or expected services on a system or class of systems, Tripwire will alert on new, unexpected ports. Report generation is automated once the solution is fully implemented, and allows for reporting as often as is desired.

## Evidence Reporting

Report by asset

### Services - Documentation [Windows]

Reference (Windows Server)

Services - Documentation [Windows] (Command Output Capture Rule)

#### Local Services

Version : 8/27/14 2:35 PM

Type : Modified

#### Content

Justification for each allowed service

Service: AeLookupSvc  
Description: Microsoft Windows Application Experience  
Justification: Core Windows Component  
Last Reviewed by: David Thornton  
Last Reviewed date: 05/16/2013

Service: ALG  
Description: Microsoft Windows Application Layer Gateway Service  
Justification: Core Windows Component  
Last Reviewed by: David Thornton  
Last Reviewed date: 05/16/2013

Service: AppHostSvc  
Description: Microsoft Windows Application Host Helper Service  
Justification: Core Windows Component  
Last Reviewed by: David Thornton  
Last Reviewed date: 05/16/2013

The solution has built-in options which allow for:

- » Specifying justification by individual servers or by server role
- » Custom fields

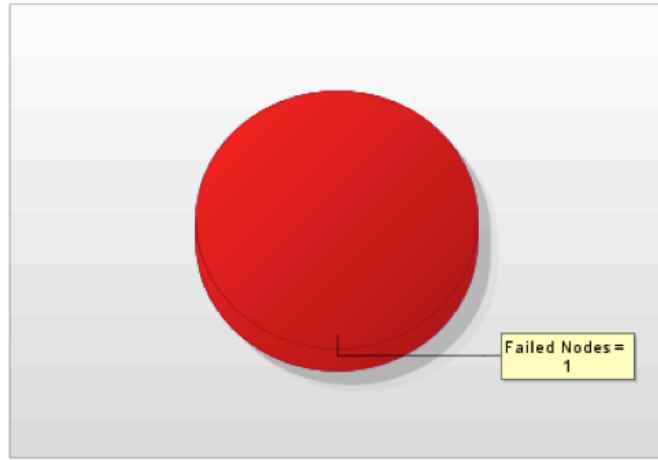
## Support and Requirements

This solution is supported on:

- » Windows
- » RHEL
- » AIX
- » Solaris

# Compliance Alerting

## Services



● Failed Nodes

Ensure No Unauthorized Services Are Running [Windows]

<u>Node</u>	<u>Passed Tests</u>	<u>Failed Tests</u>	<u>Percent Compliant</u>
Reference	0	1	0%

Drill-down on an asset to show details of unexpected services

## Drilldown - Detailed Test Results

Ensure No Unauthorized Services Are Running [Windows]

*The Responsible Entity shall enable only those ports and service*

**Node: Reference (Windows Server)**

**Overall result: Failed @ 9/18/14 6:21 PM**

**Element: Unauthorized Local Services**

### Result

Failed

### Time

9/18/14 6:21 PM

### Actual

Unauthorized services=

```
*****  
** UNAUTHORIZED SERVICE FOUND **  
*****  
Service: gupdate
```

```
*****  
** UNAUTHORIZED SERVICE FOUND **  
*****  
Service: gupdatem
```

Return to a compliant state by stopping or justifying the service



## PLATFORM COVERAGE AND REQUIREMENTS

All solution areas listed in the chart below are based on Tripwire Enterprise. All server platforms require Tripwire Enterprise v8.0 or later and a Tripwire Enterprise agent installed on the server.

PLATFORM	PORT	SERVICES	USERS	SOLUTION AREA				
				USERS & PASSWORDS	GROUPS	SOFTWARE	SHARES	ROUTES
Windows <sup>1</sup>	X	X	X	X	X	X	X	X
RHEL <sup>2</sup>	X	X	X	X		X		X
AIX 5.3 <sup>3</sup>	X	X	X			X		
AIX 6.1 <sup>3</sup>	X	X	X			X		
Solaris 10 <sup>3,4</sup>	X	X	X			X		
NMAP Scans <sup>5</sup>	X							

Additional platforms can be supported through a custom engagement with Tripwire Professional Services.

<sup>1</sup> Windows XP, 7, 8, 2000, 2003, 2008, 2008 R2 & 2012

<sup>2</sup> Requires WGET or CURL

<sup>3</sup> Requires LSOF and WGET

<sup>4</sup> Global Zone only

<sup>5</sup> Requires NMAP capable host with TE Agent to act as initiator



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at [tripwire.com](https://tripwire.com)**

***The State of Security: News, trends and insights at [tripwire.com/blog](https://tripwire.com/blog)***  
**Connect with us on [LinkedIn](#), [Twitter](#) and [Facebook](#)**