



 **Trustwave**[®]
Smart security on demand

Secure Web Gateway SNMP Monitoring and TW MIB

Legal Notice

Copyright © 2014 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave.

While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:

Phone: +1.800.363.1621

Email: support@trustwave.com

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Revision History

| Version | Date | Changes |
|---------|--------------|-------------------------|
| 1.0 | October 2013 | First Trustwave version |
| 2.0 | June 2014 | Update |

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

| Formats and Symbols | Meaning |
|--------------------------|--|
| Blue Underline | A blue underline indicates a Web site or email address. |
| Bold | Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes. |
| Code | Text in <code>Courier New 9 pt in blue</code> indicates computer code or information at a command line. |
| Italics | Italics denotes the name of a published work, the current document, name of another document, text emphasis, to introduce a new term, and path names. |
| [Square brackets] | Square brackets indicate a placeholder for values and expressions. |

Notes, Tips, and Cautions



Note: This symbol indicates information that applies to the task at hand.



Tip: This symbol denotes a suggestion for a better or more productive way to use the product.



Caution: This symbol highlights a warning against using the software in an unintended manner.



Question: This symbol indicates a question that the reader should consider.

About This Guide

This document details the current Trustwave Secure Web Gateway MIB (Management Information Base) as at June 2014.

Table of Contents

| | |
|---|-----|
| Legal Notice | ii |
| Trademarks | ii |
| Revision History | ii |
| Formatting Conventions | iii |
| Notes, Tips, and Cautions | iii |
| About This Guide | iv |
| 1 Introduction — SNMP and TrustwaveSWG | 5 |
| 2 SNMP and Alerts | 6 |
| 2.1 SNMP Configuration | 7 |
| 3 Management Information Base — General | 10 |
| 3.1 Using a Standard MIB | 10 |
| 3.2 Object Identifier (OID) | 10 |
| 3.3 Example Using a Non-Standard OID | 11 |
| 4 Trustwave SWG MIB | 12 |
| 4.1 MIB Entries | 12 |
| 4.2 Values for OID 1.3.6.1.4.1.6790.1.1.100.1.1.2.0 | 18 |
| 4.3 3rd Party Entries | 20 |
| 4.3.1 Third Party Supplied OIDs for Trustwave MIB | 20 |

1 Introduction — SNMP and TrustwaveSWG

The Simple Network Management Protocol (SNMP) is an application-layer Internet protocol designed to facilitate the exchange of management and monitoring information between network devices.

SNMP enables network administrators to manage network performance, find and solve network problems, and plan network capacity and growth.

Secure Web Gateway enables:

- sending SNMP traps
- replying to SNMP queries based on either:
 - a dedicated Trustwave SWG MIB (Management Information Base)
 - basic Linux system MIBs
- using SNMPv2c or SNMPv3.

SNMP is one of two methods that can be used for event Alerts in the Secure Web Gateway. (The other method is email.)

For security reasons, Trustwave does NOT support using SNMP to configure network devices.

A MIB definition file, called TRUSTWAVESWG-MIB.txt, is available from the Trustwave website. This file should be imported into your SNMP monitoring software.

2 SNMP and Alerts

Alerts provide an important mechanism for monitoring the main modules and components of the system. Through the Alerts mechanism, SWG can notify you of system events, application events, update events, and security events.

The following table indicates the alerts included in each type of event.

| Event Type | Alerts |
|---------------------------|---|
| System Events | Hard Drive Threshold, System Load, Memory Usage Threshold |
| Application Events | Emergency Policy Selected, Archive Upload Failed, Backup Failed, Log Handler Down, Scanning Process is Unexpectedly Down, License Expiry, License Modification or Update, Active / Standby Policy Server, No Connection to Policy Server for Past Hour. Security Updates are Not Installed! Connection to Policy Server Restored, Connection to Email Server Failed |
| Update Events | OS Update Available, Security Update Available, Security Update Failed, OS Update Failed, Security Update Successfully Installed, OS Update Successfully Installed, Could Not Download the Update File, Error in Validating Checksum, Update Failed due to Internal Error, Received Update with Unsupported Version, Update Exceeded Maximum Installation Time, Could not find the Update File, The Update File was not Created Properly, Update Installed Successfully, OS Update Available, Security Updates Available, Update Added to Available Updates, Update already Installed, Update already Exists, A Later Version of Update Exists, Installing Update, Update Dependence Problem, All Scanners in the topology must have the same VSOS as Policy Server before you start Update Process, Update Installer - Cannot install OS Update when Standby Policy Server VSOS is different from Active Policy Server Version |
| Security Settings | Anti-Virus triggered (settings configurable), Behavior Analysis (settings configurable), Blocked URL List (settings configurable) URL Filtering (settings configurable) |

SWG can send alerts through two different communication methods (besides System Log messages):

- Email messages
- SNMP notification.

These methods must be enabled before they can be used for sending alert notifications. For alert notification to use SNMP, you must configure SNMP settings.



To enable alerts, you should configure how alerts will be sent (SNMP/Email) for each event type (System/Application/Update/Security). You do this in the **Alerts Settings** window.

To assign Alert methods to Event types:

1. Select **Administration | Alerts | Alert Settings**. The Alert Settings window is displayed.
2. Click **Edit**.
3. For each type of Event, check the alert notification method (SNMP and/or Email).



- Email alerts are enabled only if the **Enable Sending Email** check box in **Administration | System Settings | Mail Server** is checked.
- SNMP alerts are enabled only if the **Enable Trap Sending** check box in **Administration | Alerts | SNMP Settings** is checked.

4. For each event type for which you requested email alerts, specify the target email address. To specify more than one email address for an event type, click the  icon, and select **Add Row**.
5. Click **Save**.
6. If you configured SNMP alerts to be sent, follow the [To configure the SNMP settings](#) procedure.
7. If you are ready to distribute and implement the changes in your system devices, click .

2.1 SNMP Configuration

If your site will be using SNMP alerts, you need to configure SNMP settings. As part of this task, you can enable and configure MIB Monitoring and SNMP Trap Sending:

- MIB (Management Information Base) is a database of objects that can be monitored by the network management system (SNMP). This collection of information is organized hierarchically and comprises managed objects identified by object identifiers.
- SNMP traps are deployed as a means of notifying the management station of specific events by way of an SNMP message.

SWG supports SNMP v2.c and SNMP v3.

Both versions support MIB Monitoring and SNMP Traps Sending, but SNMP v3 provides greater security by securing device access for MIB Monitoring and SNMP Trap Sending through authentication and encryption over the network. (SNMPv3 mandates that trap messages are rejected unless the SNMPv3 user sending the trap is defined in the user database of the management console.)

Therefore, when configuring SNMP v3, you define a number of configuration parameters relating to authentication, privacy, and access control.

SNMP configuration settings are defined in the SNMP Settings window. This window contains two tabs:

General — In this tab, you configure the SNMP protocol for MIB Monitoring/Trap sending, as well as the ports. You also configure the Hostname/IP destination servers for receiving the SNMP traps.

SNMP Version — In this tab, you select with which version of SNMP the system will work, and define any needed parameters.

To configure SNMP settings:

1. Select **Administration | Alerts | SNMP Settings**.

The General tab of the SNMP Settings window is displayed. In this tab, you configure the SNMP protocol for MIB Monitoring/Trap sending, as well as the ports. You also configure the Hostname/IP destination servers for receiving the SNMP traps.

2. Click **Edit**.
3. To enable SWG to perform MIB monitoring, ensure that the **Enable MIB Monitoring** check box is selected, and in the **Listening Port (input)** field, specify the port (default: 161) against which SWG should perform SNMP queries.
4. To enable SWG to send traps, ensure that the **Enable Trap Sending** check box is selected, and in the **Trap Port (output)** field, specify the corresponding Trap Port (default: 162).
5. If the Policy server should be the Trap Destination Server, click the **Set Policy server as Trap Destination Servers** check box.
6. In the three entry fields to the right of the associated check boxes, optionally specify up to three possible destination servers.

If the device is set up to query a Domain Name System (DNS) server, you are permitted to specify a host name instead of an IP address for the trap destination.

To have the traps sent to any or all of these servers, select the check box beside the server.

7. Select the SNMP Version tab. In this tab, you select with which version of SNMP the system will work, and define any needed parameters.
8. Choose the SNMP version, and do one of the following as appropriate:
 - If you selected SNMPv2.c, in the Community field define the group to which the devices and management stations running SNMP belong. (Default string: "Trustwave"). Then skip to Step 10.
 - If you selected SNMPv3:
 - a. Define the SNMP MIB Monitoring parameters, as follows.



The Monitoring parameters define the security protocol and encryption methods used to obtain information from the SNMP agent on the machine. The information retrieved is part of a MIB.

- i. In the **Security Name** field, specify the SNMP user name.
- ii. In the **Security Level** field, select whether the messages should be sent unauthenticated (None), authenticated, or authenticated and encrypted.
- iii. If you specified that the messages should be sent unauthenticated (that is, you specified None), skip to Step b below. If you specified that the Security Level should include authentication (that is, you specified a value other than None), fill in the remaining parameters in the **SNMP MIB Monitoring** area as instructed in the following substeps.
- iv. In the **Authentication Protocol** field, select the Authentication Protocol — either **MD5** or **SHA** (verification checksums).

- v. In the **Authentication Key** field, specify the user's authentication key, which signs the message being sent. (Minimum: 8 characters.)
- vi. In the **Encryption Key** field, specify the user's encryption key, which encrypts the data portion of the message being sent. (Minimum: 8 characters.)




The encryption mode or privacy protocol used is DES (encryption algorithm).

- b. Define the SNMP Traps parameters, by doing either of the following:



SNMPv3 mandates that trap messages are rejected unless the SNMPv3 user sending the trap already exists in the user database. The user database in a SNMPv3 application is referenced by a combination of the user's name (Security Name) and an automatically supplied identifier for the given SNMP application (engineID).

- To supply the same Security parameters (name, level, etc.) for SNMP Traps that you used for MIB Monitoring, click the **Use SNMP MIB Monitoring information** check box.
 - Otherwise, fill in a **Security name**, **Security level**, **Authentication Protocol**, **Authentication key** and **Encryption key** for SNMP Traps (as for MIB Monitoring in Step 8a).
9. To test that the traps are successfully sent to the SNMP servers, click the **Test** button. A test message will be sent to the defined server with the SNMP name, IP and SWG Software Version.
10. Click **Save**.
11. If you are ready to distribute and implement the changes in your system devices, click .

3 Management Information Base — General

A Management Information Base (MIB) is a monitoring information list of objects that can be monitored by an SNMP Manager. A MIB is an information format that describes general information which is common to most devices.

Trustwave Secure Web Gateway supports the following SNMP MIB types:

- System MIBII
- Interfaces MIBII
- IP MIBII
- TCP MIBII
- Host Resources MIB
- Application proprietary MIB

3.1 Using a Standard MIB

Any SNMP Management software that works with SNMP can be used, such as one of the following:

- HPOV
- TEMIP
- MRTG/PRTG

3.2 Object Identifier (OID)

To maximize its monitoring capabilities, the SNMP Management System must recognize the MIBs of the managed elements in the network. The MIBs include a technical description of the Object Identifiers (OIDs) that can be managed or monitored by the Manager, which pre-loads the MIBs into memory during its initiation.

An object Identifier, also known as a MIB variable, is described by a set of concatenated numbers separated by dots which build up a unique string identifier. Each OID defines a different value from various aspects, system, application or other.

While system values are mostly supported through the standard MIB - II, the application and other values in Secure Web Gateway are exposed through Trustwave's specific (non-standard) Object IDs.

The Scanner status OIDs contain the following values:

| Application | Values |
|--|--|
| Scanner Status | 1.3.6.1.4.1.2021.8.1.100.1 Possible Values: 0: Scanner Up 1: Scanner Down |
| Scanner Status String | 1.3.6.1.4.1.2021.8.1.101.1 Possible Values: scan is Up scan is Down |

3.3 Example Using a Non-Standard OID

The following example describes how the administrator can calculate the overall average of CPU usage. Note that there are several different ways to calculate CPU usage.

To calculate CPU usage:

1. Calculate delta values for all CPU counters (deltaIdle, deltaUser, deltaNice, deltaSystem, deltaKernel) by taking a sample for each CPU counter every n amount of time.
2. Subtract the value taken at an earlier point in time from the value calculated at a later point in time to calculate the delta value.
For example, if at 10.00am, the value for CpuUser was 15, and at 10.02, the value for CpuUser was 20, then $20-15=5$.
3. Total each of the delta values for each CPU counter (delta CpuIdle + delta CpuUser + delta CpuNice + delta CpuSystem + delta CpuKernel) to obtain the deltaTotal.
The CPU Usage in percentage is $100 - 100 * \text{deltaIdle} / \text{deltaTotal}$.
This represents the CPU Usage between the sampled time intervals.

4 Trustwave SWG MIB

Trustwave has designed its own SWG MIB.

4.1 MIB Entries



Important:

- Each of the Trustwave SWG OID values in the following table is preceded by the prefix **1.3.6.1.4.1.6790**
- When the Trustwave SWG OID value ends in .x, there will be one value for each of the scanning engines within the scanner. The number of scanning engines will depend on the device type. The first scanning engine is 1.

| OID | Field | Values |
|----------------------------|---|---|
| 1.3.6.1.4.1.6790... | | |
| .1.1.2.0 | Secure Web Gateway product version | Alphanumeric string |
| .1.1.3.0 | Secure Web Gateway Build Information | Alphanumeric string |
| .1.1.10.0 | Device Type | String: All in One Scanning Server Policy Server |
| .1.1.11.0 | Machine type | Alphanumeric string |
| .1.1.30.7.1.0 | Log Handler Process ID | Integer |
| .1.1.30.7.5.0 | Last date and time the log handler data was reset | Date and Time |
| .1.1.30.7.12.1.0 | Total number of logs since last reset | Integer |
| .1.1.30.7.12.2.0 | Total number of logs sent to the logging database since last reset | Integer |
| .1.1.30.7.12.3.0 | Total number of logs sent to the archives database since last reset | Integer |
| .1.1.30.7.12.4.0 | Total number of logs sent to the reports database since last reset | Integer |
| .1.1.30.7.12.5.0 | Total number of logs sent to syslog since last reset | Integer |

| OID | Field | Values |
|-----------------------------|---|---------------|
| 1.3.6.1.4.1.6790... | | |
| .1.1.30.20.1.1.2.x | Current blocked requests per second | Integer |
| .1.1.30.20.1.1.3.x | Current emergency status of scanning engine x | Integer |
| .1.1.30.20.2.1.1.2.x | Total number of requests which were logged since last reset | Integer |
| .1.1.30.20.2.1.1.3.x | Total number of requests which were sent to the Logging database since last reset | Integer |
| .1.1.30.20.2.1.1.4.x | Total number of requests which were sent to the Archive database since last reset | Integer |
| .1.1.30.20.2.1.1.5.x | Total number of requests which were sent to the Reports database since last reset | Integer |
| .1.1.30.20.2.1.1.6.x | Total number of requests which were sent to the Syslog database since last reset | Integer |
| .1.1.30.21.1.1.3.1.x | Last date and time the scanning server data was reset | Date and Time |
| .1.1.30.21.1.1.3.2.x | Last date and time the HTTP data was reset | Date and time |
| .1.1.30.21.1.1.3.3.x | Last date and time the HTTPS data was reset | Date and time |
| .1.1.30.21.1.1.3.4.x | Last date and time the FTP data was reset | Date and time |
| .1.1.30.21.1.1.3.5.x | Last date and time the ICAP data was reset | Date and time |
| .1.1.30.21.1.1.4.1.x | Total number of requests scanned since last reset | Integer |
| .1.1.30.21.1.1.4.2.x | Total number of HTTP requests scanned since last reset | Integer |
| .1.1.30.21.1.1.4.3.x | Total number of HTTPS requests scanned since last reset | Integer |
| .1.1.30.21.1.1.4.4.x | Total number of FTP requests scanned since last reset | Integer |
| .1.1.30.21.1.1.4.5.x | Total number of ICAP requests scanned since last reset | Integer |
| .1.1.30.21.1.1.5.1.x | Average rate of requests scanned per second | Integer |
| .1.1.30.21.1.1.5.2.x | Average rate of HTTP requests scanned per second | Integer |
| .1.1.30.21.1.1.5.3.x | Average rate of HTTPS requests scanned per second | Integer |
| .1.1.30.21.1.1.5.4.x | Average rate of FTP requests scanned per second | Integer |
| .1.1.30.21.1.1.5.5.x | Average rate of ICAP requests scanned per second | Integer |

| OID | Field | Values |
|----------------------------|---|---------|
| 1.3.6.1.4.1.6790... | | |
| .1.1.30.21.1.1.6.1.x | Total input scanned since last reset | Integer |
| .1.1.30.21.1.1.6.2.x | Total HTTP input scanned since last reset | Integer |
| .1.1.30.21.1.1.6.3.x | Total HTTPS input scanned since last reset | Integer |
| .1.1.30.21.1.1.6.4.x | Total FTP input scanned since last reset | Integer |
| .1.1.30.21.1.1.6.5.x | Total ICAP input scanned since last reset | Integer |
| .1.1.30.21.1.1.7.1.x | Total output scanned since last reset | Integer |
| .1.1.30.21.1.1.7.2.x | Total HTTP output scanned since last reset | Integer |
| .1.1.30.21.1.1.7.3.x | Total HTTPS output scanned since last reset | Integer |
| .1.1.30.21.1.1.7.4.x | Total FTP output scanned since last reset | Integer |
| .1.1.30.21.1.1.7.5.x | Total ICAP output scanned since last reset | Integer |
| .1.1.30.21.1.1.8.1.x | Total number of requests which were blocked since last reset | Integer |
| .1.1.30.21.1.1.8.2.x | Total number of HTTP requests which were blocked since last reset | Integer |
| .1.1.30.21.1.1.8.3.x | Total number of HTTPS requests which were blocked since last reset | Integer |
| .1.1.30.21.1.1.8.4.x | Total number of FTP requests which were blocked since last reset | Integer |
| .1.1.30.21.1.1.8.5.x | Total number of ICAP requests which were blocked since last reset | Integer |
| .1.1.30.21.1.1.9.1.x | Total number of requests which were blocked due to Virus detection since last reset | Integer |
| .1.1.30.21.1.1.9.2.x | Total number of HTTP requests which were blocked due to Virus detection since last reset | Integer |
| .1.1.30.21.1.1.9.3.x | Total number of HTTPS requests which were blocked due to Virus detection since last reset | Integer |
| .1.1.30.21.1.1.9.4.x | Total number of FTP requests which were blocked due to Virus detection since last reset | Integer |
| .1.1.30.21.1.1.9.5.x | Total number of ICAP requests which were blocked due to Virus detection since last reset | Integer |
| .1.1.30.21.1.1.10.1.x | Total number of requests which were blocked due to Behavior analysis since last reset | Integer |

| OID | Field | Values |
|------------------------------|---|---------|
| 1.3.6.1.4.1.6790... | | |
| .1.1.30.21.1.1.10.2.x | Total number of HTTP requests which were blocked due to Behavior analysis since last reset | Integer |
| .1.1.30.21.1.1.10.3.x | Total number of HTTPS requests which were blocked due to Behavior analysis since last reset | Integer |
| .1.1.30.21.1.1.10.4.x | Total number of FTP requests which were blocked due to Behavior analysis since last reset | Integer |
| .1.1.30.21.1.1.10.5.x | Total number of ICAP requests which were blocked due to Behavior analysis since last reset | Integer |
| .1.1.30.21.1.1.11.1.x | Total number of requests which were blocked due to being Blacklisted since last reset | Integer |
| .1.1.30.21.1.1.11.2.x | Total number of HTTP requests which were blocked due to being blacklisted since last reset | Integer |
| .1.1.30.21.1.1.11.3.x | Total number of HTTPS requests which were blocked due to being blacklisted since last reset | Integer |
| .1.1.30.21.1.1.11.4.x | Total number of FTP requests which were blocked due to being blacklisted since last reset | Integer |
| .1.1.30.21.1.1.11.5.x | Total number of ICAP requests which were blocked due to being blacklisted since last reset | Integer |
| .1.1.30.21.1.1.12.1.x | Total number of requests which were blocked due to URL category since last reset | Integer |
| .1.1.30.21.1.1.12.2.x | Total number of HTTP requests which were blocked due to URL category since last reset | Integer |
| .1.1.30.21.1.1.12.3.x | Total number of HTTPS requests which were blocked due to URL category since last reset | Integer |
| .1.1.30.21.1.1.12.4.x | Total number of FTP requests which were blocked due to URL category since last reset | Integer |
| .1.1.30.21.1.1.12.5.x | Total number of ICAP requests which were blocked due to URL category since last reset | Integer |
| .1.1.30.21.1.1.13.1.x | Total number of requests blocked due to Data Leakage Prevention (DLP) since last reset. | Integer |
| .1.1.30.21.1.1.13.2.x | Total number of requests blocked due to Data Leakage Prevention (DLP) since last reset. | Integer |

| OID | Field | Values |
|------------------------------|---|---------|
| 1.3.6.1.4.1.6790... | | |
| .1.1.30.21.1.1.13.3.x | Total number of requests blocked due to Data Leakage Prevention (DLP) since last reset. | Integer |
| .1.1.30.21.1.1.13.4.x | Total number of requests blocked due to Data Leakage Prevention (DLP) since last reset. | Integer |
| .1.1.30.21.1.1.13.5.x | Total number of requests blocked due to Data Leakage Prevention (DLP) since last reset. | Integer |
| .1.1.30.40.1.0 | Total open HTTP and HTTPS connections | Integer |

Note: The following OIDs deal with SNMP Trap variable bindings

.1.1.100.2.0 An alarm has been set or cleared in the Secure Web Gateway system.

Possible Variable Bindings:

vsAlarmEventType

vsAlarmProbableCause

vsAlarmSpecificProblems

vsAlarmSeverity

vsAlarmAdditionalText

vsAlarmProposedRepairActions

vsAlarmServerName

vsAlarmServerIP

vsAlarmServerInetAddress

vsAlarmServerInetAddressType



Note: From SWG 11.6, vsAlarmServerIP is replaced by:

- vsAlarmServerInetAddress – Addresses in either IPv4 or IPv6 format.
- vsAlarmServerInetAddressType – Values of 2, 1, or 0, representing addresses of type IPv6, IPv4, or an empty string respectively.

vsAlarmServerVersion

vsAlarmServerType

vsAlarmEventTime

| OID | Field | Values |
|---------------------|-------|--------|
| 1.3.6.1.4.1.6790... | | |

Note: The following rows deal, in succession, with the above Alarm variable bindings.

| | | |
|------------------|---|---|
| .1.1.100.1.1.1.0 | Represents the EventType values for the alarms Possible Values (integers): 1 = Other 2 = Communications Alarm 3 = Quality of Service Alarm 4 = Processing Error Alarm 5 = Equipment Alarm 6 = Environmental Alarm 7 = Integrity Violation 8 = Operational Violation 9 = Physical Violation 10 = Security Service or Mechanism Violation 11 = Time Domain Violation | |
| .1.1.100.1.1.2.0 | Represents the Probable Cause values for the alarms. For possible values, see the next section. | |
| .1.1.100.1.1.3.0 | Represents the Specific Problems field for the alarm | Integer |
| .1.1.100.1.1.4.0 | Represents the perceived Severity values for the alarms | Integer where: 1 = Cleared 2 = Indeterminate 3 = Critical 4 = Major 5 = Minor 6 = Warning |
| .1.1.100.1.1.5.0 | Represents the Additional Text field for the alarm | Alphanumeric string |
| .1.1.100.1.1.6.0 | Represents the Proposed Repair Actions field for the alarm | Alphanumeric string |
| .1.1.100.1.1.7.0 | Secure Web Gateway Server Name | Alphanumeric string |

| OID | Field | Values |
|----------------------------|---|---------------------|
| 1.3.6.1.4.1.6790... | | |
| .1.1.100.1.1.8.0 | Secure Web Gateway Server IP | IP address |
| .1.1.100.1.1.9.0 | Secure Web Gateway Server Version | Size |
| .1.1.100.1.1.10.0 | Secure Web Gateway Server Type (Scanning, Policy, etc) | Alphanumeric string |
| .1.1.100.1.1.11.0 | Secure Web Gateway Event Date and Time (GMT) | Date and Time |

4.2 Values for OID 1.3.6.1.4.1.6790.1.1.100.1.1.2.0

This table represents the **Probable Cause** values for the alarms. The columns list the possible values (integers).

| Value | Value | Value |
|--|------------------------------------|--------------------------------------|
| 1 = Other | 26 = LAN error | 51 = Temperature Unacceptable |
| 2 = Adapter Error | 27 = Leak Detected | 52 = Threshold Crossed |
| 3 = Application Subsystem Failure | 28 = Local Node Transmission Error | 53 = Timing Problem |
| 4 = Bandwidth Reduced | 29 = Loss of Frame | 54 = Toxic Leak Detected |
| 5 = Call Establishment Error | 30 = Loss of Signal | 55 = Transmit Failure |
| 6 = Communication Protocol Error | 31 = Material Supply Exhausted | 56 = Transmitter Failure |
| 7 = Communication Subsystem Failure | 32 = Multiplexer Problem | 57 = Underlying Resource Unavailable |
| 8 = Configuration or Customization Error | 33 = Out of Memory | 58 = Version Mismatch |
| 9 = Congestion | 34 = Output Device Error | 59 = Authentication Failure |
| 10 = Corrupt Data | 35 = Performance Degraded | 60 = Breach of Confidentiality |
| 11 = CPU Cycles Limit Exceeded | 36 = Power Problem | 61 = Cable Tamper |
| 12 = Data Set or Modem Error | 37 = Pressure Unacceptable | 62 = Delayed Information |
| 13 = Degrade Signal | 38 = Processor Problem | 63 = Denial of Service |
| 14 = dte Dce Interface Error | 39 = Pump Failure | 64 = Duplicate Information |
| 15 = Enclosure Door Open | 40 = Queue Size Exceeded | 65 = Information Missing |
| | 41 = Receive Failure | 66 = Information Modification |

| Value | Value | Value |
|--|---|----------------------------------|
| 16 = Equipment Malfunction | 42 = Receiver Failure | Detected |
| 17 = Excessive Vibration | 43 = Remote Node Transmission Error | 67 = Information out of Sequence |
| 18 = File Error | 44 = Resource at or nearing Capacity | 68 = Intrusion Detection |
| 19 = Fire Detected | 45 = Response Time Excessive | 69 = Key Expired |
| 20 = Flood Detected | 46 = Retransmission Rate Excessive | 70 = Non Repudiation Failure |
| 21 = Framing Error | 47 = Software Error | 71 = Out of Hours Activity |
| 22 = Heating Vent Cooling System Problem | 48 = Software Program Abnormally Terminated | 72 = Out of Service |
| 23 = Humidity Unacceptable | 49 = Software Program Error | 73 = Procedural Error |
| 24 = Input Output Device Error | 50 = Storage Capacity Problem | 74 = Unauthorized Access Attempt |
| 25 = Input Device Error | | 75 = Unexpected Information |

4.3 3rd Party Entries



Important: The following OIDs provided with the Trustwave Secure Web Gateway MIB are supplied by a third party (Squid). Therefore, they have a DIFFERENT prefix than Trustwave-supplied OIDs. The prefix of the following OIDs is 1.3.6.1.4.1.3495.

4.3.1 Third Party Supplied OIDs for Trustwave MIB

| OID | Field | Values |
|---------------------|---|---------|
| 1.3.6.1.4.1.3495... | | |
| .1.1.2.0 | Cache Disk | Integer |
| .1.3.1.3.0 | Cache Memory Usage | Integer |
| .1.3.2.2.1.9.5 | Cache Hit Ratio | Integer |
| .1.3.2.1.5 | Total volume of KBs sent back to the users per requests | Integer |

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com>.