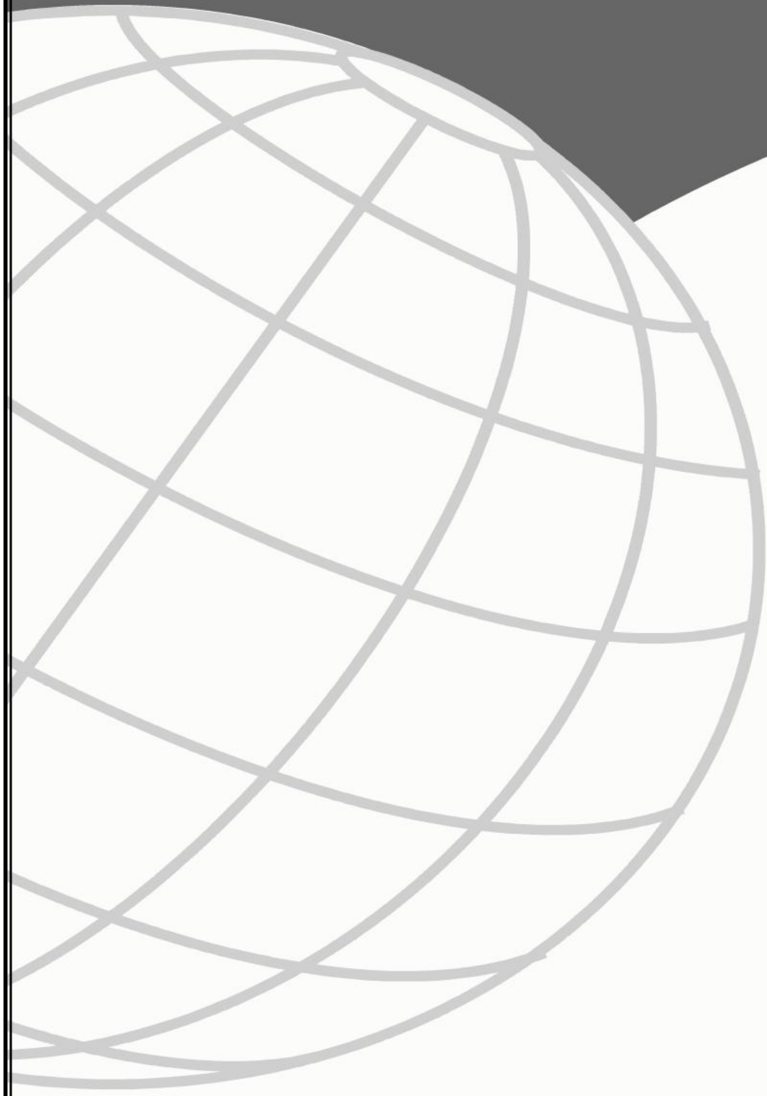


Enabling Service Excellence

Monitoring SiteMinder Environments

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

©2014 eG Innovations Inc. All rights reserved.

Table of Contents

Table of Figures

Chapter

1

Introduction

SiteMinder is a platform for secure portal, extranet, and intranet management. It meets key authentication, authorization, and personalization requirements for building and managing secure Web sites. A SiteMinder installation consists of two main components: the *SiteMinder Policy Server* and the *SiteMinder Agent*. The Policy Server manages the access control policies established by an administrator. These policies define which resources are protected and which users or user groups are allowed access to resources. Using policies, an administrator can set time constraints on resource availability and IP address constraints on the client attempting access. The Policy Server runs on an NT or UNIX system and performs key security and portal management operations. To meet the security needs of each environment, the Policy Server supports a range of authentication methods and uses existing directory services to authenticate users. By supporting a wide range of authentication methods, the Policy Server provides flexibility and security for a diverse set of users. A SiteMinder Agent integrates with a Web server, a Web application server, or a custom application to enforce access control based on pre-defined policies.

Figure 1.1 illustrates a simple implementation of a SiteMinder Policy Server in a SiteMinder environment (that includes a single SiteMinder Web Agent).

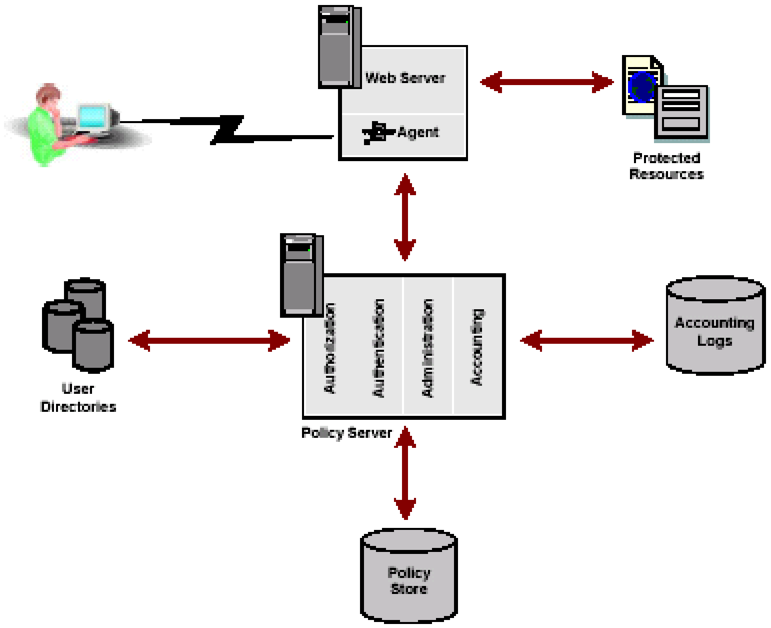


Figure 1.1: SiteMinder system overview

In a Web implementation, a user requests a resource through a browser. That request is received by the Web Server and intercepted by the SiteMinder Web Agent. The Web Agent determines whether or not the resource is protected, and if so, gathers the user's credentials and passes them to the Policy Server. The Policy Server authenticates the user against native user directories, then verifies if the authenticated user is authorized for the requested resource based on rules and policies contained in the Policy Store. Once a user is authenticated and authorized, the Policy Server grants access to protected resources and delivers privilege and entitlement information.

A problem in even a single step of this process could expose web sites to malicious virus attacks. It is therefore imperative that the SiteMinder environment is continuously monitored for security leaks.

eG Enterprise provides different ways of monitoring the SiteMinder environment. For instance, eG agents can be deployed on each of the systems hosting a Web agent. Since every Web agent writes operational statistics to a local log file, the eG agent deployed on a Web agent host parses the log files and reads the desired performance data.

Alternatively, the eG agent can be deployed on the Policy server itself. In this case, the eG agent uses SNMP to draw meaningful performance metrics from a component named **SiteMinder OneView Monitor**, which is hosted by the Policy server. This component identifies performance bottlenecks and provides information about resource usage in a SiteMinder deployment by collecting operational data from the Policy server and the Web agent. Each machine that hosts a monitored component includes an OneView agent, which sends operational data to the OneView Monitor.

Figure 23.2 illustrates how the OneView Monitor is integrated in a SiteMinder deployment, and how the eG agent pulls performance data from the OneView Monitor.

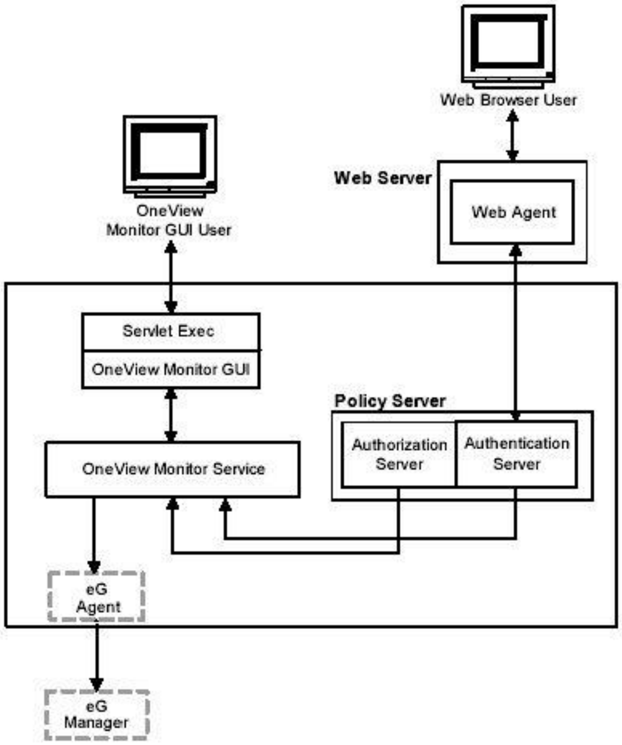


Figure 1.2: SiteMinder and OneView Monitor

Depending upon the mode of monitoring that best suits their needs, users can adopt either one of the following monitoring models presented by the eG Enterprise suite:

- the *SiteMinder Policy* model where monitoring is done by parsing log files, or
- the *SiteMinder 1view* model, where monitoring is done using the SiteMinder OneView monitor

This document discusses both these models extensively.

Chapter

2

Monitoring the SiteMinder Environment using Log Files

Using the *SiteMinder Policy* server model depicted by Figure 2.1, the eG agent executes a wide variety of tests that continuously track the availability of the SiteMinder environment and effectively evaluate the performance of each of the crucial services offered by the environment.

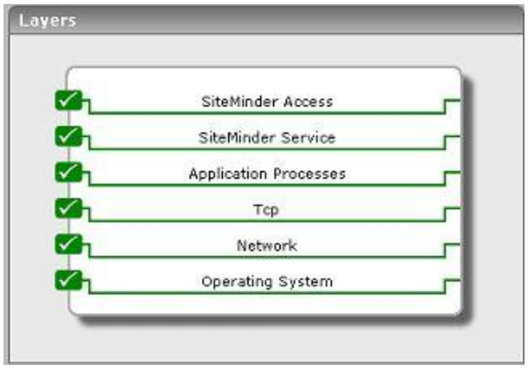
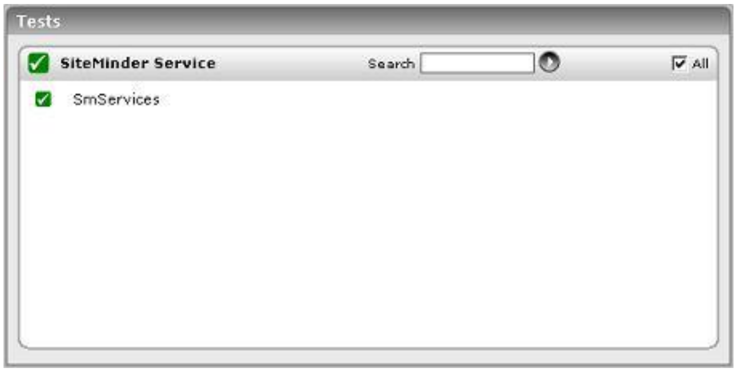


Figure 2.1: Layer model of a SiteMinder 5.5 (or below)

Since the bottom 4 layers of Figure 2.1 have already been discussed in the *Monitoring Unix and Windows Servers* document, the sections that follow will discuss the top 2 layers only.

2.1 The SiteMinder Service Layer

The **SiteMinder Service** layer (see Figure 2.3) reports the availability of the Policy server and measures the time taken by the Policy server to perform authorization and authentication checks.


Tests

☑ SiteMinder Service

Search

☑ All

☑ SmServices

Figure 2.2: The test associated with the SiteMinder Service layer

2.1.1 SmServices Test

The SmServices test measures the availability of the SiteMinder Policy Server services (Authentication, Authorization, Accounting, and Administration), and the time taken by the policy server for performing authentication and authorization checks.

Purpose	Measures the availability of the SiteMinder Policy Server services, and the time taken by the policy server for performing authentication and authorization checks
Target of the test	A SiteMinder Policy server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port at which the server listens 4. **timeout -** The duration (in seconds) for which the test should wait for a response from the policy server services 5. **authenticationport** - The port number of the Authentication Service of the Policy server 6. **authorizationport** - The port number of the Authorization Service of the Policy server 7. **accountingport** - The port number of the Accounting service of the Policy server 8. **adminport** - The port number of the Administration service of the Policy server 9. **agentname** - The name of the configured webagent in the policy server user interface 10. **sharedsecret** - The shared secret assigned to the specified web agent 11. **resource** - The resource, which is protected by the above configured web agent and requires username and password for authentication. Example: "/transpolar/inventory/3inventorysignon.htm". While specifying the resource value, ensure that it does not contain the IP address of the host machine. An example for a wrong resource value would be: "http://192.168.10.47/transpolar/inventory/3inventorysignon.htm" 12. **action** – The action that needs to be checked. Example: "GET” 13. **username** - A valid **USERNAME** having permissions for the specified resource and configured action 14. **password** - The password for the above user 15. **jarfilepath** - The full path to the directory in which the "smjavaagentapi.jar" file is present (this file is part of a SiteMinder installation). 16. **detailed diagnosis** - To make diagnosis more efficient and accurate, the eG Enterprise system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular component, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: ▪ The eG manager license should allow the detailed diagnosis capability ▪ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.		
Outputs of the test	One set of results for every SiteMinder Policy server being monitored.		
Measurements made by the	Measurement	Measurement Unit	Interpretation

test	**Authentication port status:** The status of the Authentication service running on the given port.	Percent	A value of 100 for this measure indicates that the service is running. A 0 value indicates that the service is down.
	Authorization port status: The status of the Authorization service running on the given port.	Percent	A value of 100 for this measure indicates that the service is running. A 0 value indicates that the service is down.
	Accounting port status: The status of the Accounting service running on the given port	Percent	A value of 100 for this measure indicates that the service is running. A 0 value indicates that the service is down.
	Admin port status: The status of the Admin service running on the given port.	Percent	A value of 100 for this measure indicates that the service is running. A 0 value indicates that the service is down.
	User login status: The status of the user login check performed by the policy server.	Percent	A value of 100 for this measure indicates that the configured user for this test is authenticated. A 0 value indicates that the authentication process failed.
	User login time: Time taken by the policy server to perform a login check.	Secs	
	User authorization status: The status of the user authorizatiin check performed by the policy server	Percent	A value of 100 for this measure indicates that the configured user for this test is authorized for the configured resource. A 0 value indicates that the authorization process failed.
	User authorization time: Time taken by the policy server for performing the authorization check	Secs	

	Total time: Total time taken by the test for initialization of agent api object, for connecting to the policy server, checking whether the configured resource is protected or not, authentication check, authorization check and for uninitialization of the agent api object.	Secs	

To know the Administration, Accounting, Authorization, and Authentication ports of the SM Policy server, do the following:

1. Open the **SiteMinder Policy Server Management Console** using the menu sequence depicted by Figure 2.3 below:

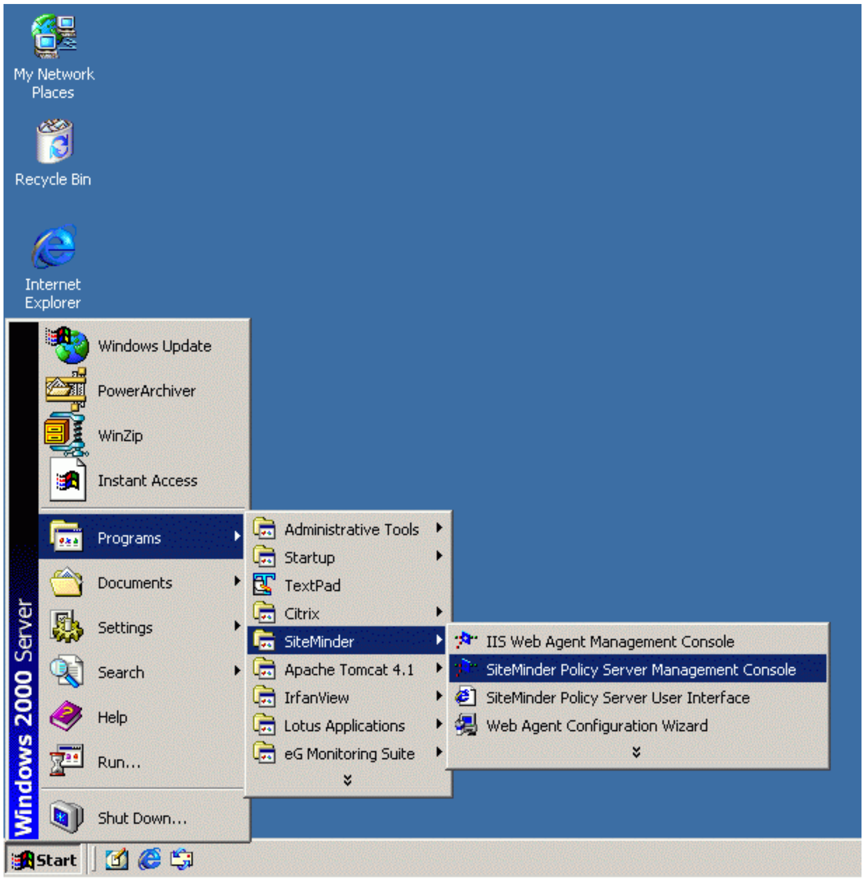
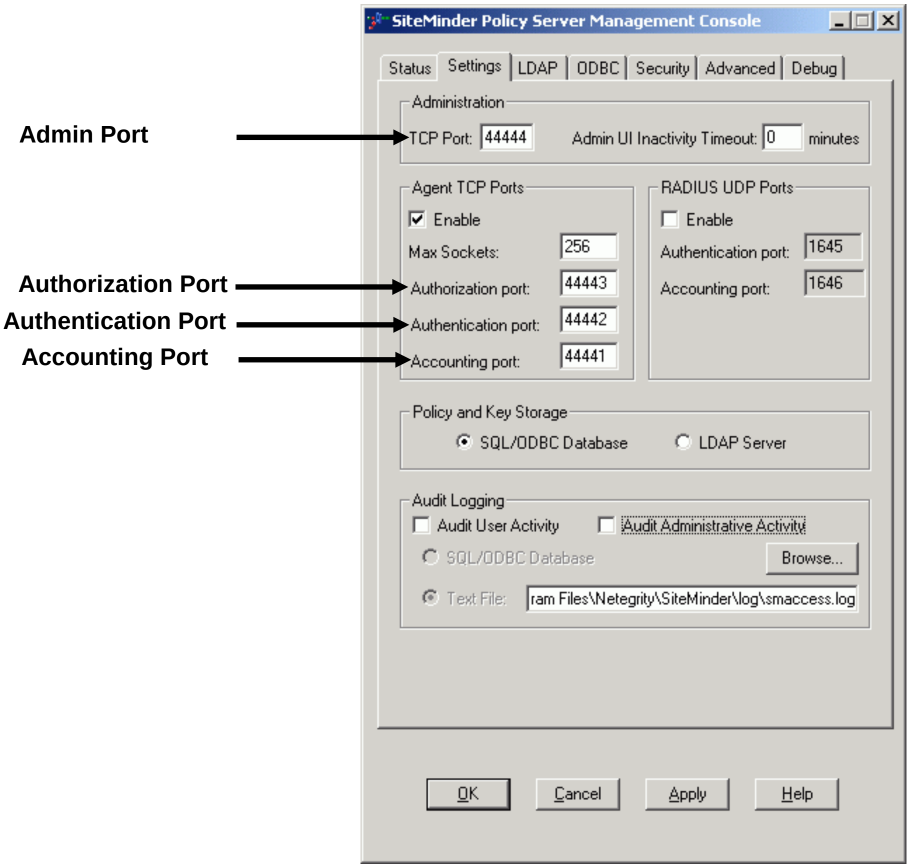


Figure 2.3: Opening the SiteMinder Policy Server Management Console

2. Click on the **Settings** tab in the **SiteMinder Policy Server Management Console** to view the TCP ports of the policy server services (see Figure 2.4).


Admin Port

Authorization Port

Authentication Port

Accounting Port

SiteMinder Policy Server Management Console

Administration

TCP Port: 44444 Admin UI Inactivity Timeout: 0 minutes

Agent TCP Ports

☑ Enable

Max Sockets: 256

Authorization port: 44443

Authentication port: 44442

Accounting port: 44441

RADIUS UDP Ports

□ Enable

Authentication port: 1645

Accounting port: 1646

Policy and Key Storage

● SQL/ODBC Database ○ LDAP Server

Audit Logging

□ Audit User Activity □ Audit Administrative Activity

○ SQL/ODBC Database

● Text File: ram Files\Netegrity\SiteMinder\log\smaccess.log

Figure 2.4: Viewing the service ports

2.2 The SiteMinder Access Layer

This layer uses the tests depicted by Figure 2.5 to track the admin logins to the policy server, and assess the efficiency of the authorization and authentication operations performed by the server.

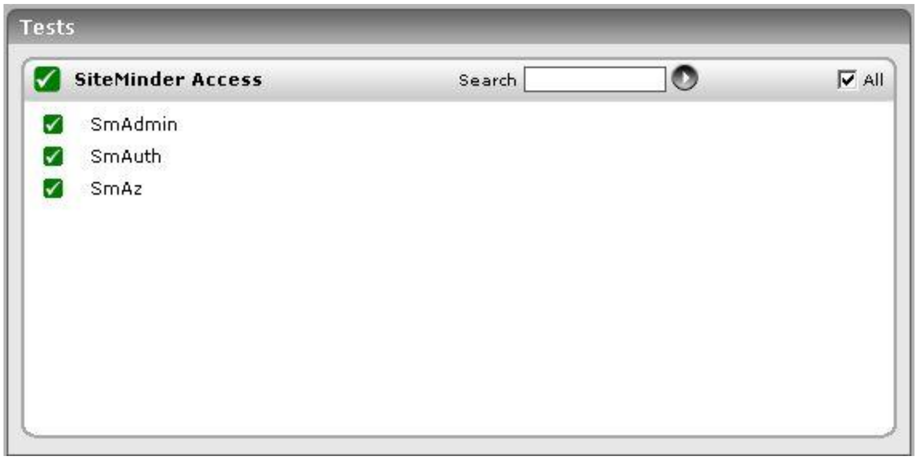


Figure 2.5: The tests associated with the SiteMinder Access layer

2.2.1 SmAdmin Test

The SmAdmin test reports statistics pertaining to the administrator logins to the policy server.

Purpose	Reports statistics pertaining to the administrator logins to the policy server
Target of the test	A SiteMinder Policy server
Agent deploying the test	An internal agent

<table>
<tr><td><b>Configurable parameters for the test</b></td><td colspan="3">1. <b>TEST PERIOD</b> - How often should the test be executed
2. <b>Host</b> - The host for which the test is to be configured.
3. <b>port</b> – The port number of the administration service (see Figure 2.4) in the policy server
4. <b>logoption</b> - Currently, this test collects measures by parsing the log files. Therefore, specify "logFile" as the <b>logoption</b>. Future versions of eG may include support for database logging.
5. <b>path</b> - The full path to the log file. For example, "D:\Progra~1\Netegrity\SiteMinder\Log\smaccess.log".
6. <b>agentnames</b> – A comma-separated list of agent names
7. <b>detailed diagnosis</b> - To make diagnosis more efficient and accurate, the eG Enterprise system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular component, choose the <b>On</b> option against <b>DETAILED DIAGNOSIS</b>. To disable the capability, click on the <b>Off</b> option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
- The eG manager license should allow the detailed diagnosis capability
- Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for every SiteMinder Policy server being monitored.</td></tr>
<tr><td rowspan="3"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Admin logins:</b>
The number of successful administrator logins during the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td><b>Admin login rejects:</b>
The number of administrator login rejects during the last measurement period.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, provides the details of the administrator logins that were rejected by the SM Policy server</td></tr>
<tr><td></td><td><b>Percent admin login rejects:</b>
The percentage of administrator login rejects during the last measurement period.</td><td>Percent</td><td></td></tr>
</table>

2.2.2 SmAuth Test

The SmAuth test reports statistics pertaining to the user authentications to the policy server.

Purpose	Reports statistics pertaining to the user authentications to the policy server		
Target of the test	A SiteMinder Policy server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the authentication service (see Figure 2.4) in the policy server 4. **logoption** - Currently, this test collects measures by parsing the log files. Therefore, specify "logFile" as the **logoption**. Future versions of eG may include support for database logging. 5. **path** - The full path to the log file. For example, "D:\Progra~1\Netegrity\SiteMinder\Log\smaccess.log". 6. **agentnames** – A comma-separated list of agent names 7. **detailed diagnosis** - To make diagnosis more efficient and accurate, the eG Enterprise system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular component, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: ▪ The eG manager license should allow the detailed diagnosis capability ▪ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.		
Outputs of the test	One set of results for every SiteMinder Policy server being monitored.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Authentication accepts: The number of users successfully authenticated by the policy server during the last measurement period.	Number	

	Authentication rejects: The number of user authentications rejected by the policy server during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, provides the details of the authentication attempts that were rejected by the SM Policy server.
	Authentication attempts: The number of authentication attempts failed during the last measurement period.	Number	
	Authentication challenges: The number of authentication challenges during the last measurement period.	Number	
	Authentication rejects percent: The percentage of authentication rejects during the last measurement period.	Percent	
	Authentication attempts percent: The percent of authentication attempts during the last measurement period.	Percent	

2.2.3 SmAz Test

The SmAz test reports statistics pertaining to the user authorizations to the policy server.

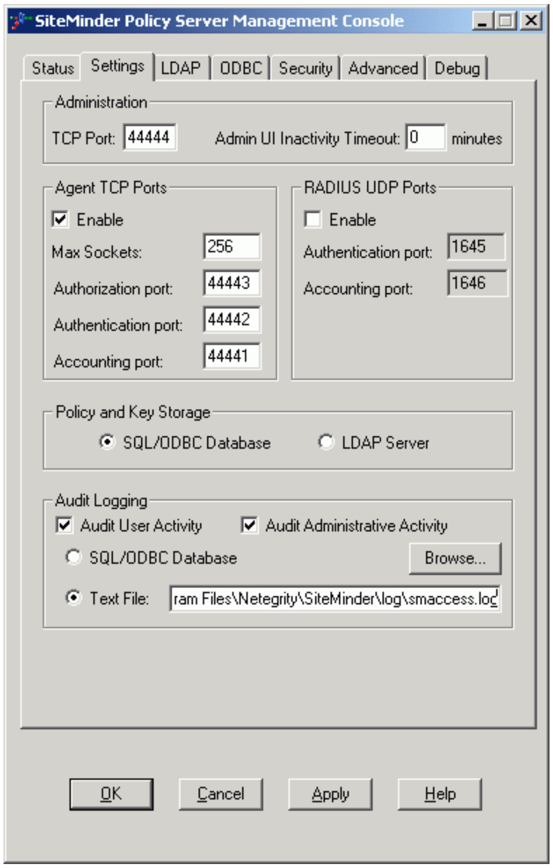
Purpose	Reports statistics pertaining to the authorizations to the policy server
Target of the test	A SiteMinder Policy server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the authorization service (see Figure 2.4) in the policy server 4. **logoption** - Currently, this test collects measures by parsing the log files. Therefore, specify "logFile" as the **logoption**. Future versions of eG may include support for database logging. 5. **path** - The full path to the log file. For example, "D:\Progra~1\Netegrity\SiteMinder\Log\smaccess.log". 6. **agentnames** – A comma-separated list of agent names 7. **detailed diagnosis** - To make diagnosis more efficient and accurate, the eG Enterprise system embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular component, choose the **On** option against **DETAILED DIAGNOSIS**. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: ▪ The eG manager license should allow the detailed diagnosis capability ▪ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.		
Outputs of the test	One set of results for every SiteMinder Policy server being monitored.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Authorization accepts: The total number of users authorized to access the resource during the last measurement period.	Number	
	Authorization rejects: The total number of users not authorized to access the resource during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, provides the details of the authorization attempts that were rejected by the SM Policy server.
	Authorization rejects pct: The percentage of authorization rejects during the last measurement period.	Percent	

In order to ensure that the SmAdmin test, SmAuth test, and SmAz test function effectively, audit logging has to be enabled for the SiteMinder policy server. To achieve this, do the following:

1. Open the "SiteMinder Policy Server Management Console" using the menu sequence depicted by Figure 2.3.

2. Click on the **Settings** tab to open it.



Administration
TCP Port: 44444 Admin UI Inactivity Timeout: 0 minutes

Agent TCP Ports
☑ Enable
Max Sockets: 256
Authorization port: 44443
Authentication port: 44442
Accounting port: 44441

RADIUS UDP Ports
□ Enable
Authentication port: 1645
Accounting port: 1646

Policy and Key Storage
● SQL/ODBC Database ○ LDAP Server

Audit Logging
☑ Audit User Activity ☑ Audit Administrative Activity
○ SQL/ODBC Database
● Text File: ram Files\Netegrity\SiteMinder\log\smaccess.log

Figure 2.6: Enabling audit logging

3. In the **Audit Logging** section present at the bottom of this tab (see Figure 2.6), click on the **Audit User Activity** and **Audit Administrative Activity** check boxes.

4. Then, select the **Text File** option, and specify the full path to the log file that is to be used for audit logging. Ensure that the same path is specified against the **PATH** parameter of the SmAdminTest, SmAuthTest, and SmAzTest, respectively.

5. Finally, click the **Apply** button and then the **OK** button to register the changes.

2.2.4 SmAuthLog Test

The SmAuthLog test monitors the authentications to the SiteMinder policy server by parsing the debug log file. This test is disabled by default. To enable the tests, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *SiteMinder Policy* as the **Component type**, set *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Purpose	Monitors the authentications to the SiteMinder policy server by parsing the debug log file		
Target of the test	A SiteMinder Policy server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the policy server 4. **logfile -** Provide the absolute name of the SiteMinder debug log file.		
Outputs of the test	One set of results for every SiteMinder Policy server being monitored.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Successful logins: Indicates the number of successful logins during the last measurement period.	Number	
	Failed logins: Indicates the number of failed logins during the last measurement period.	Number	
	Login failure percent: Indicates the percentage of failed logins during the last measurement period.	Percent	

2.2.5 SmAzLog Test

The SmAzLog test monitors the authorizations to the SiteMinder policy server by parsing the debug log file. This test is disabled by default. To enable the tests, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *SiteMinder Policy* as the **Component type**, set *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Purpose	Monitors the authorizations to the SiteMinder policy server by parsing the debug log file		
Target of the test	A SiteMinder Policy server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the policy server 4. **logfile -** Provide the absolute name of the SiteMinder debug log file.		
Outputs of the test	One set of results for every SiteMinder Policy server being monitored.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Authorization accepts: Indicates the number of requests accepted during the last measurement period.	Number	
	Authorization rejects: Indicates the number of requests rejected during the last measurement period.	Number	
	Authorization rejects percent: Indicates the percentage of requests rejected during the last measurement period.	Percent	

Chapter

3

Monitoring the SiteMinder Environment using the OneView Monitor

The *SiteMinder 1view* monitoring model (see Figure 3.1) gives an integrated view of the entire SiteMinder infrastructure including the Policy servers and Web agents.

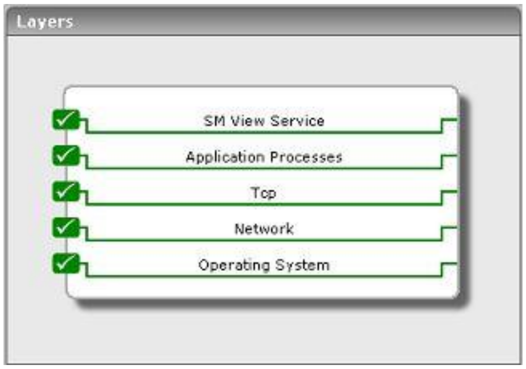


Figure 3.1: Layer model of the SiteMinder 1view server

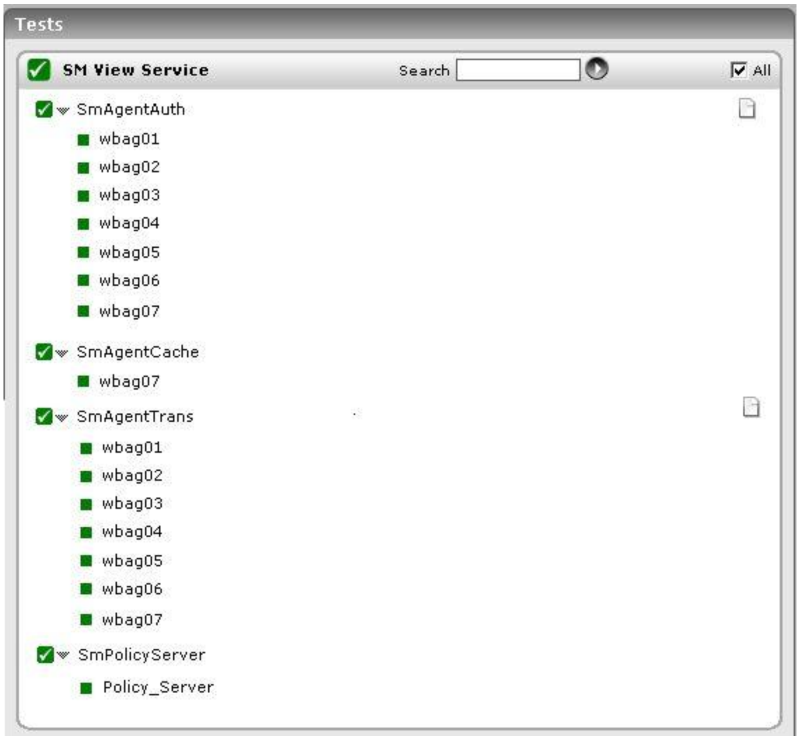
As the bottom 4 layers of Figure 3.1 have been discussed at length in the *Monitoring Unix and Windows Servers* document, the sections to come will elaborate on the **SM View Service** layer only.

3.1 The SM View Service Layer

This layer tracks the complete gamut of services offered by the SiteMinder environment, which includes (see Figure 3.2):

- Authentication
- Authorization
- Cache management

- Making IsProtected calls to the Policy server



Tests

☑ SM View Service Search ☑ All

- ☑ SmAgentAuth
  - wbag01
  - wbag02
  - wbag03
  - wbag04
  - wbag05
  - wbag06
  - wbag07
- ☑ SmAgentCache
  - wbag07
- ☑ SmAgentTrans
  - wbag01
  - wbag02
  - wbag03
  - wbag04
  - wbag05
  - wbag06
  - wbag07
- ☑ SmPolicyServer
  - Policy_Server

Figure 3.2: The tests associated with the SM View Service layer

3.1.1 SmAgentAuth Test

This test tracks every critical step in the request authorization cycle of a Web agent, beginning with the Web agent's attempt to login to the Policy server, through the request validation process, and finally, authorization. In the process, it indicates if any serious errors/failures have occurred at any stage.

Purpose	Monitors the authorizations to the SiteMinder policy server using SNMP
Target of the test	The Policy Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the Policy server 4. **snmpport** - The port number at which the Policy server exposes its SNMP MIB. The default is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the Policy server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every Web agent that reports measurements to the OneView Monitor on the Policy server		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Login calls: Indicates the number of login attempts made by this Web agent during the last measurement period.	Number	
	Login errors: Indicates the number of errors that occurred during the login attempts made in the last measurement period.	Number	An error indicates a communication failure between the Web agent and the Policy server. Therefore, a very high value of this measure could indicate a problem condition requiring investigation.
	Login failures: Indicates the number of failed login attempts during the last measurement period.	Number	A login attempt can fail if users are not authorized or authenticated by the Policy server.
	Login time: Indicates the time taken by the user to log into a resource.	Secs	Ideally, this value should be low.

	Validation calls: Indicates the number of times, in the last measurement period, this Web agent attempted to validate a session cookie against the Policy server to authenticate a user, instead of matching the user's credentials to a user directory entry.	Number	The Web Agent creates a session cookie on the user’s browser when a user is successfully authenticated, and uses that cookie to authenticate the user on subsequent requests for new resources. The following conditions affect this measure: ➢ **User Session Cache size**—If a Web Agent’s user session cache is set to a value greater than 0, the user’s session information is stored in the cache. The Web agent validates the session against the session cache instead of the Policy server, so the value of this measure does not increase. If the user session cache is set to 0, this measure increases each time a user requests a protected resource because the Web agent must validate the session against the Policy Server. ➢ **Multi-thread vs. Multi-process cache**—Web agents that use multi-threaded cache, such as IIS Web Agents, iPlanet 4.x and 6.0 Web Agents (on Windows operating systems, and Domino Web Agents (on Windows and UNIX operating systems), add a session to the session cache (if the session cache size is greater than 0) when a user is successfully authenticated. If that user requests additional resources from the same realm, the Web agent validates the user against the session cache, so the Validation_calls measure does not increase. Apache and iPlanet 4.x and 6.0 Web Agents running on UNIX operating systems, which use multi-process cache, do not add the session cookie to the session cache until the user presents the cookie to the Web agent during a request for another resource in the realm where she was authenticated. The Web agent validates the first request made with a session cookie against the Policy Server, which increases the ValidationCount. Subsequent requests are validated against the cache.

	Validation errors: Indicates the number of errors that occurred when this Web agent attempted to validate a user session during the last measurement period.	Number	Errors indicate a communication failure between the Web agent and the Policy server. A high value of this measure therefore, is indicative of a problem.
	Validation failures: Indicates the number of times, in the last measurement period, this Web Agent has failed to validate a user session because of an invalid session cookie.	Number	Ideally, this value should be low.
	Validation success percent: Indicates the percentage of validation attempts that were successful, currently.	Percent	A high success percentage is an indicator of good health.
	Validation time: Indicates the time this Web agent takes to validate a cookie used to authenticate a user.	Secs	Ideally, this value should be low.
	Authorization calls: Indicates the number of authorization attempts made by this Web Agent during the last measurement period.	Number	An authorization attempt occurs when a user supplies credentials to the Policy Server in order to access a protected resource.
	Authorization errors: Indicates the number of errors that occurred during authorization attempts made by this Web Agent during the last measurement period.	Number	An error indicates a communication failure between the Web Agent and Policy Server during an authorization call.
	Authorization failures: Indicates the failed authorization attempts during the last measurement period.	Number	An authorization attempt fails when a user enters invalid credentials.

	Authorization success percent: Indicates the percentage of authorization attempts that were currently successful.	Percent	
	Authorization time: Indicates the average time it takes to authorize a user.	Secs	Ideally, this value should be low.

3.1.2 SmAgentCache Test

SiteMinder provides several caches that can be configured to maintain copies of recently accessed data (for example, user authorizations) to improve system performance. These caches should be configured to suit the nature of the data in your environment, but may also require periodic manual flushing. SiteMinder deployments can be configured to maintain the following cache on the Policy Server:

- **User Authorization Cache**—Stores user distinguished names (DNs) based on the user portion of policies and includes the users' group membership.

SiteMinder also maintains an *Agent Cache* on each SiteMinder Agent machine. The Agent Cache has two components:

- **Agent Resource Cache**—Stores a record of accessed resources that are protected by various realms. This cache speeds up Agent to Policy Server communication, since the Agent knows about resources for which it has already processed requests.
- **Agent User Cache**—Maintains users' encrypted session tickets. It acts as a session cache by storing user, realm, and resource information. Entries in this cache are invalidated based on timeouts established by the realms a user accesses.

The **SmAgentCache** test monitors the performance of the *Agent Cache*.

Purpose	Monitors the performance of the *Agent Cache*
Target of the test	The Policy Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the policy server 4. **snmpport** - The port number at which the Policy server exposes its SNMP MIB. The default is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the Policy server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every Web agent that reports measurements to the OneView Monitor on the Policy server		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Resource cache hits percent: Indicates the percentage of times the resource cache is accessed by this Web agent.	Percent	The value of this measure is indicative of how frequently SiteMinder uses cached resources. Higher the value of this measure, better will be the system performance. A very low value of this measure on the other hand, could cause slow-downs in the Web agent to Policy server communication.
	Session cache hits percent: Indicates the percentage of times this Web agent accessed the user session cache.	Percent	A high value of this measure speeds up resource requests, whereas a low value slackens its pace.

3.1.3 SmAgentTrans Test

Web agents place IsProtected calls on the Policy server to check whether a resource is protected or not. This test monitors such IsProtected calls.

Purpose	Monitors the **IsProtected** calls issued by the Web agent to the Policy server
Target of the test	The Policy Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the policy server 4. **snmpport** - The port number at which the Policy server exposes its SNMP MIB. The default is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the Policy server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every Web agent that reports measurements to the OneView Monitor on the Policy server		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Resource protect calls: Indicates the number of times in the last measurement period, the Web agent has checked the Policy server to see if a resource is protected.	Number	If the resource cache is adequately sized, then the value of this measure can be kept at a healthy minimum. For instance, if the resource cache is set to 0, two or more IsProtected calls may be recorded per login attempt. If the Web agent is not caching information, it must check with the Policy server to determine whether or not a resource is protected each time a request is made to the Web server. If the resource cache is not set to 0, only one IsProtected call will be recorded. In this case, the Web agent makes one IsProtected call to the Policy server; subsequent requests to the Web server for the same resource are satisfied against the Web agent's resource cache until the resource in the cache expires or the resource cache is flushed.
	Resource protect errors: Indicates the number of times during the last measurement period, an error occurred when the Web agent asks the Policy server whether or not a resource is protected.	Number	A high value of this measure could indicate a high incidence of communication failures between the Web agent and the Policy server.
	Resource protect time: The average amount of time it takes for the Web agent to determine from the Policy server whether or not a resource is protected.	Secs	Ideally, this value should be low.

	Cross site script hits: Indicates the number of cross-site scripting hits that occurred during the last measurement period.	Number	Ideally, this value should be 0. Any value higher than that indicates the existence of malicious code in some pages of your site.
	Bad url character hits: Indicates the number of requests that this Web agent refused during the last measurement period, because of bad URL characters.	Number	Bad URL characters are specifically blocked to prevent a Web client from evading SiteMinder rules. These characters are specified in the Web agent's configuration. Ideally, this value should be low. A very high value could either indicate the frequent usage of bad URL characters in requests, or a misconfiguration of the Web agent.
	Bad cookie hits: Indicates the number of cookies that this Web agent could not decrypt in the last measurement period.	Number	
	Expire cookie hits: Indicates the number of requests that contained an expired cookie in the last measurement period.	Number	

3.1.4 SmPolicyServer Test

This test monitors the authentication and authorization attempts made by every Web agent on the Policy server, and reveals the number of successful/failed attempts.

Purpose	Monitors the authentication and authorization attempts made by every Web agent on the Policy server
Target of the test	The Policy Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port number of the policy server 4. **snmpport** - The port number at which the Policy server exposes its SNMP MIB. The default is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the Policy server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every Web agent that reports measurements to the OneView Monitor on the Policy server		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Connection accepts: Indicates the number of TCP connections currently open between this Web agent and the Policy server.	Number	
	Authentication accepts: Indicates the number of successful authentications performed by the Policy server during the last measurement period.	Number	
	Authentication rejects: Indicates the number of failed authentication attempts during the last measurement period.	Number	
	Authentication accepts percent: Indicates the percentage of successful authentications on the Policy server.	Percent	
	Authorization accepts: Indicates the number of successful authorizations during the last measurement period.	Number	

	Authorization rejects: Indicates the number of authorization attempts that failed during the last measurement period.	Number	
	Authorization accepts percent: Indicates the percentage of successful authorizations performed by the Policy server.	Percent	

Chapter

4

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to **SiteMinder environments**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.