Layer 7 Technologies
Secure Installation Guide

Contents

Introduction

This guide describes how to configure the Layer 7 SecureSpan SOA Gateway v8.0 for secure installation, to conform to Common Criteria requirements.

Prerequisites

This guide assumes that the SecureSpan SOA Gateway v8.0 has been set up and configured according to the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

A correctly configured SOA Gateway largely conforms to the evaluated configuration. The remainder of this document provides additional information.

Evaluated Configuration

The evaluated configuration is achieved once the Layer 7 SOA Gateway v8.0 is configured according to the *Layer 7 Installation and Maintenance Manual (Appliance Edition).*

Note the following:

- Hardware Security Modules (either PCI or network) may be optionally installed on the Gateway appliance.
- The browser client version of the Policy Manager may not be used.

Objectives for Operational Environment

This section describes the objectives for the Policy Manager operational environment and any additional steps you must take to achieve these objectives.

Table 1: Operational environment objectives (ESM Policy Manager PP)

Identifier	Description	Specific configuration required?
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.	None. Assigning administrators to the operational environment is covered by the topics “Managing Roles” and “Adding a User or Group to a Role”.
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data.	None. Configuring a remote location for audits is described in the topic “Managing the Audit Sink”.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a secure manner.	None.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	None.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.	None.
OE.USERID	The Operational Environment must be able to identify a user requesting access to the TOE.	None. Logging in to the Gateway is described in the topic “Connecting to the Gateway”.

Table 2: Operational environment objectives (ESM Access Control PP)

Identifier	Description	Specific configuration required?
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data.	None. Configuring a remote location for audits is described in the topic "Managing the Audit Sink".
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	None.
OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce	None. Configuring policies is described in the topic "Working with Service Policies".
OE.PROTECT	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.	None.
OE.USERID	The Operational Environment must be able to identify the user and convey validation of this to the TOE.	None. User is validated when logging into the Gateway—see topic "Connecting to the Gateway".
OE.TIME	The Operational Environment must provide a reliable timestamp to the TOE.	None. Use of timestamps is described in the topics "Add Timestamp Assertion" and "Require Timestamp Assertion".

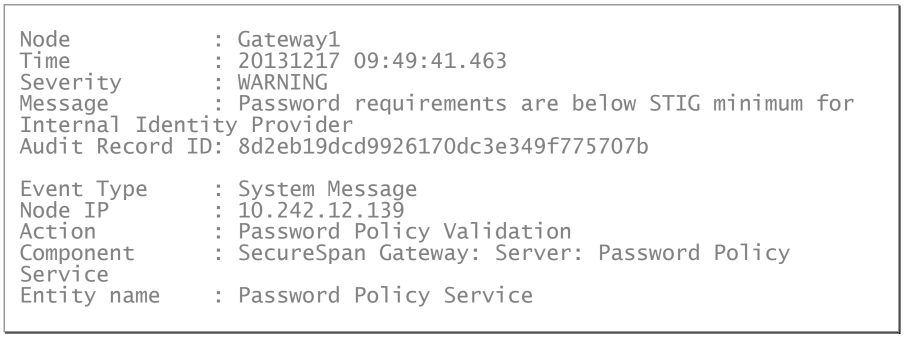
Security Requirements

This section describes any additional configuration required to meet the security requirements for Common Criteria.

Auditing

The Gateway will display an event in the Gateway Audit Viewer whenever a user is added or removed from management roles (see Appendix A on page 8). (FAU_GEN.1)

The Gateway will audit changes to password policies. When the password policy is altered from the default 'STIG' settings, the following audits are generated and are available in the Gateway Audit Events window: (FAU_GEN.1)



```
Node           : Gateway1
Time           : 20131217 09:49:41.463
Severity       : WARNING
Message        : Password requirements are below STIG minimum for
Internal Identity Provider
Audit Record ID: 8d2eb19dcd9926170dc3e349f775707b

Event Type     : System Message
Node IP        : 10.242.12.139
Action         : Password Policy Validation
Component      : SecureSpan Gateway: Server: Password Policy
Service
Entity name    : Password Policy Service
```

To enable auditing on the Gateway, add the *Audit Messages in Policy* assertion into the service policy. To disable auditing, remove this assertion from the policy. (FAU_GEN.1.1)

Information about the audit events can be view in the Gateway Audit Events window (see “Gateway Audit Events” in the *Layer 7 Policy Manager User Manual*). (FAU_GEN.1.2, FCO_NRR.2.2)

The auditing subsystem in the Layer 7 SOA Gateway involves a complex interaction between the configuration of the *Audit Messages in Policy* assertion and several cluster properties. For more information, see “Message Auditing” in the *Layer 7 Policy Manager User Manual*.

Older audit records (non-SEVERE events older than 7 days) can be purged using the Gateway Audit Events windows. The deletion of audit records is restricted only to those who have the Administrator or Gateway Maintenance roles[1]. (FAU_STG.1.1)

When connection to a repository is lost, the Gateway will stop writing to the Syslog. When connection is restored, the Gateway will resume writing to the Syslog. For brief outages, the logged information is cached on the Gateway until connection is restored. (FAU_STG_EXT.1)

Audits can also be archived using the FTP Audit Archiver feature. For more information, refer to the following topics in the *Layer 7 Policy Manager User Manual*:

FTP Audit Archiver
Audit Archiver Cluster Properties (used to configure thresholds, etc.)

Audit events may be logged to an internal Gateway database file or to an external Syslog server. For information on how to configure this, see “Managing Log Sinks” in the *Layer 7 Policy Manager User Manual.* (FAU_STG_EXT.1.1)

[1] Note that the Gateway Maintenance role by itself will not allow this—a user would need other roles that allow cluster node information to be read, such as “Manage <*name*> Service” or “Operator”.

Administrative User Account Configuration

Configure the password requirements as necessary using the Manage Password Policy task (under Tasks > Manage Account Policies in the Policy Manager). The minimum password length should be 16. (FIA_SOS.1.1)

Configure various other user account settings such as maximum login attempts, lockout duration, and session expiry period using the Manage Administrative User Account Policy task (under Tasks > Manage Account Policies in the Policy Manager). (FIA_AFL.1.1, FIA_AFL.1.2, FTA_SSL_EXT.1.1, FTA_SSL.3.1)

For more information, refer to the following topics in the *Layer 7 Policy Manager User Manual:*

Managing Password Policy
Managing Administrative User Account Policy

Audits for Changes to Password Policies

When a password policy is changed, the following audits are recorded to the log:

```
INFO      IdentityProviderPasswordPolicy
#0000000000000000fffffffffffffffe updated (changed serializedProps)
Log:
INFO    1655        com.l7tech.server.admin:
IdentityProviderPasswordPolicy #0000000000000000fffffffffffffffe
updated (changed serializedProps)

Upon changing password policy if password policy is below STIG
Requirement (doesn't matter if before the change whether the policy
is STIG or not):
WARNING           Password requirements are below STIG minimum for
Internal Identity Provider
Log:
WARNING           59           com.l7tech.server: Password
requirements are below STIG minimum for Internal Identity Provider
```

Note that the numbers next to the severity levels are line numbers, not audit code numbers, and may be subject to change. (FIA_SOS.1.1)

User Authentication/Identification

To authenticate and identity a user in a policy, insert one of the following authentication assertions into the policy: (FIA_UAU.2, FIA_UID.2)

Authenticate Against Identity Provider Assertion
Authenticate User or Group Assertion

For more information about these assertions, see the *Layer 7 Policy Authoring User Manual*.

Security Roles

The Gateway comes with a set of predefined roles that you can assign to users to control access to the system. These are defined in the topic "Predefined Roles and Permissions" in the *Layer 7 Policy Manager User Manual.* (FMT_MSA.1(1), FMT_MSA.1(2))

Create custom roles control access to audits, log sinks, and service policies. Only authorized personnel should have access to these. For more information, see "Managing Roles" in the *Layer 7 Policy Manager User Manual*. (FMT_MOF.1(1), FMT_MOF.1(2))

Note: Be especially careful about which users get the roles Administrator and Operator. These roles have the ability to query the entire system. (FMT_MOF_EXT.1)

Replay Detection

To protect against replay attacks, add the *Protect Against Message Replay* assertion to your policy.

For more information, see "Protect Against Message Replay Assertion" in the *Layer 7 Policy Authoring User Manual.* (FPT_RPL.1)

Time Stamps

To insert a signed timestamp element to the SOAP security header of all target messages, add the *Add Timestamp* assertion to your policy. To enforce the presence of a timestamp in the target message, add the *Require Timestamp* assertion to the policy.

For more information, see the following in the *Layer 7 Policy Authoring User Manual.* (FPT_STM.1):

Add Timestamp Assertion
Require Timestamp Assertion

Secure Transport via TLS

To ensure transport-level confidentiality and integrity, include the *Require SSL or TLS Transport* assertion in your policy.

For more information, see "Require SSL or TLS Transport Assertion" in the *Layer 7 Policy Authoring User Manual.* (FTP_ITC.1.1(1), FTP_ITC.1(2))

Cryptographic Suites

The Layer 7 SOA Gateway can be configured to use third-party cryptographic suites. (FTP_TRP.1.1)

Note: To enable FIPS-compliant cryptographic algorithms, you need to set the *security.fips.enabled* cluster property to “true”. For details, see “Miscellaneous Cluster Properties” in the *Layer 7 Policy Manager User Manual*.

Appendix A: Audits for Management Role Changes

The Gateway will log the following audits whenever a user is added to or removed from a management role. These audits are visible in the Gateway Audit Event window. (FAU_GEN.1)

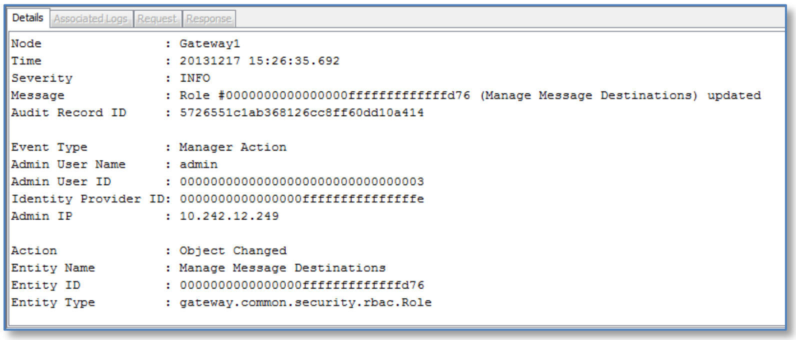
Table 3: Audits for management role changes

Role	Audit when user added to role	Audit when user removed from role
Administrator	INFO Role #0000000000000000ffffffffffffff9c (Administrator) updated	INFO Role #0000000000000000ffffffffffffff9c (Administrator) updated
Operator	INFO Role #0000000000000000ffffffffffffff6a (Operator) updated	INFO Role #0000000000000000ffffffffffffff6a (Operator) updated
Gateway Maintenance	INFO Role #0000000000000000fffffffffffffcae (Gateway Maintenance) updated	INFO Role #0000000000000000fffffffffffffcae (Gateway Maintenance) updated
Invoke Audit Viewer Policy	INFO Role #0000000000000000fffffffffffffb50 (Invoke Audit Viewer Policy) updated	INFO Role #0000000000000000fffffffffffffb50 (Invoke Audit Viewer Policy) updated
Manage [name] Folder	INFO Role #5726551c1ab368126cc8ff60dd10a345 (Manage <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a345 (Manage <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated
Manage [name] Identity Provider	INFO Role #5726551c1ab368126cc8ff60dd10a385 (Manage <IP Name> Identity Provider (#5726551c1ab368126cc8ff60dd10a383)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a385 (Manage <IP Name> Identity Provider (#5726551c1ab368126cc8ff60dd10a383)) updated
Manage [name] Policy	INFO Role #44c5f7b1aac091ea118908b01154ebee (Manage <policy name> Policy (#44c5f7b1aac091ea118908b01154ebea)) updated	INFO Role #44c5f7b1aac091ea118908b01154ebee (Manage <policy name> Policy (#44c5f7b1aac091ea118908b01154ebea)) updated
Manage [name] Service	INFO Role #5726551c1ab368126cc8ff60dd10a1b7 (Manage <Service name> Service (#5726551c1ab368126cc8ff60dd10a1b0)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a1b7 (Manage <Service name> Service (#5726551c1ab368126cc8ff60dd10a1b0)) updated
Manage Administrative Accounts Configuration	INFO Role #0000000000000000fffffffffffffb1e (Manage Administrative Accounts Configuration) updated	INFO Role #0000000000000000fffffffffffffb1e (Manage Administrative Accounts Configuration) updated

Role	Audit when user added to role	Audit when user removed from role
Manage Certificates	INFO Role #0000000000000000fffffffffffffda8 (Manage Certificates (truststore)) updated	INFO Role #0000000000000000fffffffffffffda8 (Manage Certificates (truststore)) updated
Manage Cluster Properties	INFO Role #0000000000000000fffffffffffffd44 (Manage Cluster Properties) updated	INFO Role #0000000000000000fffffffffffffd44 (Manage Cluster Properties) updated
Manage Cluster Status	INFO Role #0000000000000000fffffffffffffdda (Manage Cluster Status) updated	INFO Role #0000000000000000fffffffffffffdda (Manage Cluster Status) updated
Manage Custom Key Value Store	INFO Role #0000000000000000fffffffffffffa56 (Manage Custom Key Value Store) updated	INFO Role #0000000000000000fffffffffffffa56 (Manage Custom Key Value Store) updated
Manage Email Listeners	INFO Role #0000000000000000fffffffffffffc7c (Manage Email Listeners) updated	INFO Role #0000000000000000fffffffffffffc7c (Manage Email Listeners) updated
Manage Firewall Rules	INFO Role #0000000000000000fffffffffffffa88 (Manage Firewall Rules) updated	INFO Role #0000000000000000fffffffffffffa88 (Manage Firewall Rules) updated
Manage Internal Users and Groups	INFO Role #0000000000000000ffffffffffffff38 (Manage Internal Users and Groups) updated	INFO Role #0000000000000000ffffffffffffff38 (Manage Internal Users and Groups) updated
Manage JDBC Connections	INFO Role #0000000000000000fffffffffffffc4a (Manage JDBC Connections) updated	INFO Role #0000000000000000fffffffffffffc4a (Manage JDBC Connections) updated
Manage Listen Ports	INFO Role #0000000000000000fffffffffffffd12 (Manage Listen Ports) updated	INFO Role #0000000000000000fffffffffffffd12 (Manage Listen Ports) updated
Manage Log Sinks	INFO Role #0000000000000000fffffffffffffce0 (Manage Log Sinks) updated	INFO Role #0000000000000000fffffffffffffce0 (Manage Log Sinks) updated
Manage Message Destinations	INFO Role #0000000000000000fffffffffffffd76 (Manage Message Destinations) updated	INFO Role #0000000000000000fffffffffffffd76 (Manage Message Destinations) updated
Manage Password Policies	INFO Role #0000000000000000fffffffffffffb82 (Manage Password Policies) updated	INFO Role #0000000000000000fffffffffffffb82 (Manage Password Policies) updated
Manage Private Keys	INFO Role #0000000000000000fffffffffffffbb4 (Manage Private Keys) updated	INFO Role #0000000000000000fffffffffffffbb4 (Manage Private Keys) updated
Manage Secure Passwords	INFO Role #0000000000000000fffffffffffffbe6 (Manage Secure Passwords) updated	INFO Role #0000000000000000fffffffffffffbe6 (Manage Secure Passwords) updated
Manage UDDI Registries	INFO Role #0000000000000000fffffffffffffc18 (Manage UDDI Registries) updated	INFO Role #0000000000000000fffffffffffffc18 (Manage UDDI Registries) updated

Role	Audit when user added to role	Audit when user removed from role
Manage SiteMinder Configuration	INFO Role #0000000000000000fffffffffffffa24 (Manage SiteMinder Configuration) updated	INFO Role #0000000000000000fffffffffffffa24 (Manage SiteMinder Configuration) updated
Manage Web Services	INFO Role #0000000000000000fffffffffffffe70 (Manage Webservices) updated	INFO Role #0000000000000000fffffffffffffe70 (Manage Webservices) updated
Publish External Identity Providers	INFO Role #0000000000000000ffffffffffffff06 (Publish External Identity Providers) updated	INFO Role #0000000000000000ffffffffffffff06 (Publish External Identity Providers) updated
Publish Web Services	INFO Role #0000000000000000fffffffffffffea2 (Publish Webservices) updated	INFO Role #0000000000000000fffffffffffffea2 (Publish Webservices) updated
Search Users and Groups	INFO Role #0000000000000000fffffffffffffed4 (Search Users and Groups) updated	INFO Role #0000000000000000fffffffffffffed4 (Search Users and Groups) updated
View [name] Folder	INFO Role #5726551c1ab368126cc8ff60dd10a36b (View <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a36b (View <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated
View [name] Log Sink	INFO Role #5726551c1ab368126cc8ff60dd10a3f8 (View <log sink name> Log Sink (#5726551c1ab368126cc8ff60dd10a3f6)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a3f8 (View <log sink name> Log Sink (#5726551c1ab368126cc8ff60dd10a3f6)) updated
View Audit Records	INFO Role #0000000000000000fffffffffffffe3e (View Audit Records) updated	INFO Role #0000000000000000fffffffffffffe3e (View Audit Records) updated
View Service Metrics	INFO Role #0000000000000000fffffffffffffe0c (View Service Metrics) updated	INFO Role #0000000000000000fffffffffffffe0c (View Service Metrics) updated

Additional information is displayed about the audit when viewed in the Gateway Audit Event window. The following illustration is an example:



```
Node                : Gateway1
Time                : 20131217 15:26:35.692
Severity            : INFO
Message             : Role #0000000000000000fffffffffffffd76 (Manage Message Destinations) updated
Audit Record ID     : 5726551c1ab368126cc8ff60dd10a414

Event Type          : Manager Action
Admin User Name     : admin
Admin User ID       : 00000000000000000000000000000003
Identity Provider ID: 0000000000000000fffffffffffffffe
Admin IP            : 10.242.12.249

Action              : Object Changed
Entity Name         : Manage Message Destinations
Entity ID           : 0000000000000000fffffffffffffd76
Entity Type         : gateway.common.security.rbac.Role
```

Figure 1: Example audit in Gateway Audit Events window