PCI DSS Implementation Guide

CA API Gateway

Version 2.0

Contents

List of Figures

Chapter One: Introduction

Welcome to the Secure Implementation Document for the CA API Gateway product. This guide is intended to help customers implement CA API Management in a way that is compliant with version 2.0 of the Payment Card Industry Security Standards Council's Data Security Standards (PCI DSS).

Recommendations

This document contains only *recommendations*. Merchants and network operators are responsible for implementing their own Payment Card Industry Data Security Standards (PCI DSS) compliant environment. The purpose of this document is to assist in the secure implementation of the CA API Gateway product, by providing sufficient information regarding installation, configuration, and operation of the Gateway, to best ensure that a PCI DSS compliant environment is maintained.

Scope and Target Audience and Assumptions

This guide is intended for companies that wish to implement the CA API Gateway in accordance with guidelines set forth by the PCI DSS specifications.

This document makes many references to the *CA API Gateway Installation and Maintenance Manual*, *Policy Manager User Manual*, and the *Policy Authoring User Manual*. This document is not designed to replace the other user manuals, but rather it serves as a guide on how to configure the product using existing functionality that is documented elsewhere. It is assumed that the audience is familiar with the product line and has access to the other referenced user manuals.

PCI DSS Compliance and Validation

In 2006, American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International formed the Payment Card Industry Security Standards Council. The main purpose of the council is to produce and maintain the Data Security Standard (DSS). This is a set of rules and requirements that when followed will help prevent fraud, hacking, and other threats to private cardholder data. The main objectives of the PCI DSS are as follows:

1. Build and Maintain a Secure Network
    a. Install and maintain a firewall configuration to protect cardholder data

   b. Do not use vendor-supplied defaults for system passwords and other security parameters

2. Protect Cardholder Data
   a. Protect stored cardholder data
   b. Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program
   a. Use and regularly update anti-virus software
   b. Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
   a. Restrict access to cardholder data by business need-to-know
   b. Assign a unique ID to each person with computer access
   c. Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks
   a. Track and monitor all access to network resources and cardholder data
   b. Regularly test security systems and processes
6. Maintain an Information Security Policy
   a. Maintain a policy that addresses information security

You can find and review the complete specification by visiting the following URL: https://www.pcisecuritystandards.org/

The PCI Security Standards Council is not a compliance organization. They do not require compliance, but individual payment networks may. Visa is one such example. They require you to comply with the PCI DSS, and you must complete some degree of validation based on the annual transaction volume processed.

A qualified security assessor is the only one who can validate your PCI compliance. A current list of assessors is maintained by the PCI and can be found at this URL:

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

SPIGuard Inc. performed the compliance examination for CA Technologies. They can be contacted via any one of the following:

SPIGuard Inc.
889 West Pender St.,
Suite #703,
Vancouver, BC, V6C 3B2

Phone: 604-684-5671
FAX: 604-684-5676
http://www.spiguard.com

Chapter Two: Overview

CA Technology's award-winning family of SOA Gateways and CloudSpan Cloud Brokers allow enterprises to secure and govern the sharing of application data and functionality across organizational boundaries. Typically deployed as runtime Policy Enforcement Points (PEPs), the CA API Gateways enforce rules around how organizations interact with enterprise applications, SaaS applications and cloud-based services; as well as how third parties interact with the organization's APIs.

The CA API Gateway and development process has been certified to Common Criteria with flaw remediation, and meets all the development process requirements of that level. For more information on Common Criteria, please see http://www.commoncriteriaportal.org/.

Server Environment

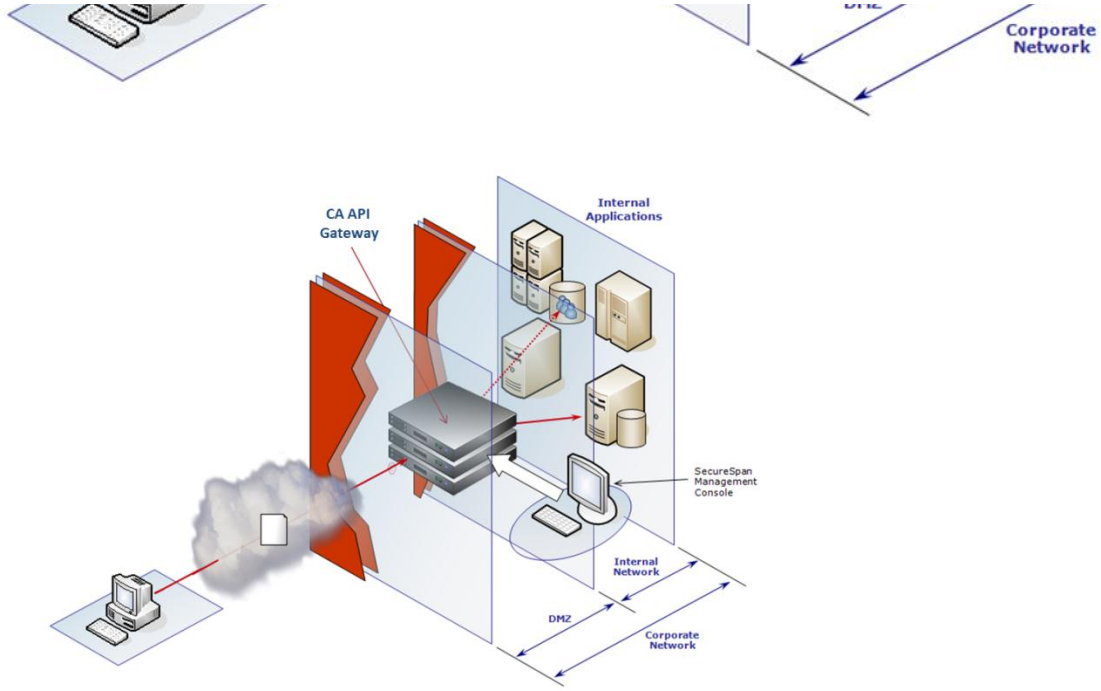

Figure 1: Server Environment

This deployment allows the Gateway to effectively secure itself and other backend systems, by dedicating network connections to specific types of traffic and restricting access to resources based on origin of network traffic. By locating inside the DMZ,

the Gateway can also be used as an effective single security boundary into the internal network.

Chapter Three: Set Up and Configure the CA API Gateway

The CA API Gateway is shipped as a hardware appliance in a "factory default" configuration. It will have an OS and Gateway installed, and will have Tarari an nCipher cards installed and ready to configure and run. Upon receiving a CA API Gateway, customers should do the following:

- Rack and power on the appliance.
- Using the Configure CA API Gateway menu, configure the operating system and network parameters.
- Using the Configure CA API Gateway menu, configure the Gateway.
- Reboot the Gateway for the configuration to take effect.

Once complete, the Gateway will be in a functioning state and ready to use.

Operating System Configuration

The Gateway is built using Red Hat Enterprise Linux as a base operating system. The OS has been customized by omitting some services, and installing but disabling some services. The Gateway has also been further locked down using DISA Application Services Security Technical Implementation Guide (STIG) V1R1, which is designed for application server products running J2EE applications. Further information on the STIG security parameters can be found at http://iase.disa.mil/stigs/stig/application-services-stig-v1r1.pdf.

The Gateway operating system environment is configurable, and may need to be modified for PCI DSS compliance, or for your particular security needs.

Services and Daemons

Appendix A lists all the services that are installed on a Gateway appliance whether they are running by default, and if they are enabled, the reason that this daemon is required is also indicated.

Some services can be disabled without impacting the functionality of the Gateway. In order to disable a service, do the following:

1. Log in to the Gateway via console or SSH.
2. From the configuration wizard, initiate a privileged shell.

3. At the root prompt, type the following:
    b. service <service name> stop
    c. chkconfig <service name> off
4. Log out.

The service is now off and will not start upon reboot.

Default usernames and username management

The Gateway operating system comes with default user accounts created with default passwords. In order to comply with PCI DSS requirements, all Gateway default passwords should be changed immediately. Further, proper internal management regarding knowledge of passwords should be followed, and system control passwords should be closely held.

Operating System root user

The root user account is the default full system administration identity for the purposes of administering the Gateway appliance. It has complete administrative control over the operating system and the services that run on it. This identity should only be used on first start of the Gateway, or when a situation warrants access to the operating system – root should not be used for regular troubleshooting issues or general access. The password should only be known to a very limited group of users, and should not be handed out to people outside that group.

The Gateway will require the root password to be reset upon first login with root. The Gateway has a default password requirement that coincides with the DISA Application Services STIG, which requires at least:

- two uppercase characters
- two lowercase characters
- two numeric characters
- two special characters
- a total of nine characters

At that time, the password must be changed to something of sufficient strength as to satisfy PCI DSS requirements.

ssgconfig user

The ssgconfig user is the default user for administering the CA API Gateway appliance. Logging into the Gateway with ssgconfig will allow users to configure the Gateway and its database, start and stop the Gateway, and provision other users to the configuration group. This credential should only be known to users that need to be able to configure the Gateway application.

Like the root user, ssgconfig will require a password change when first logging into the Gateway appliance as an ssgconfig user. The ssgconfig user has the same password strength requirements as the root user. The password must be changed to something of sufficient strength as to satisfy PCI DSS requirements.

MySQL root user

The Gateway uses a MySQL database to store configuration information pertinent to the Gateway. The database may also contain audit information and other potentially sensitive information; therefore access to the database should be restricted. The SSG process is the only process on the Gateway appliance that has regular permissions to read/write to the MySQL database, however users can get prompt access to the database via the command prompt after enabling a root session on the appliance.

The database has a root user (different from the OS-level root), that ships with a default password of '7layer'. **Unlike other passwords, the Gateway does not prompt the user to change this password upon first use, so in order to maintain PCI DSS compliance the password will have to be changed manually.** To do this:

1. Log into console as the root user.
2. Stop the Gateway process:

   ```
   service ssg stop
   ```

3. Change the password:

   ```
   mysqladmin –u root –p'oldpassword' password newpass
   ```

4. Restart the mysqld process:

   ```
   service mysqld restart
   ```

5. Start the Gateway process:

   ```
   service ssg start
   ```

When logging into the database command prompt, users will then require the root user name and password to gain access. The password should be guarded similar to the root password.

Information will be provided later in this document on how to properly protect data inside the database.

Hardware Security Module Configuration

The Gateway appliance comes optionally equipped with an nCipher nFast cryptography card and hardware security module (HSM). The HSM allows the Gateway's private key and other key material to be protected with a key stored on a secured hardware device, rather than in the database on disk or in a file on disk. CA strongly recommends use of the HSM in order to ensure PCI DSS compliance.

Please refer to CA API Gateway documentation for general instruction on using the HSM with the CA API Gateway.

Creating Keys in HSM

The HSM is normally initialized using the CA API Gateway main menu. Once initialized, two keystores will be created:

- Key for encrypting master passphrase – this key's sole purpose is to encrypt the master passphrase, which is stored in encrypted form on the Gateway file system. The master passphrase is responsible for decrypting the database password and the cluster passphrase (both in node.properties), and should not be used for any other purpose. Once created, this keystore will not appear in the CA API Gateway main menu or the Manage Keystore dialog in the Policy Manager. It is destroyed when the HSM is disabled. For more information, see the topic *Managing Keystore* in the *CA API Gateway Policy Manager User Manual*.
- Gateway SSL key – this key is the main private key used by the Gateway for accepting SSL connections, and also can act as a private key for mutual authentication on the back end.

In all cases, the key material is encrypted and can only be accessed using an HSM programmed into the same security world. Please reference the CA API Gateway documentation for further instructions on using the HSM.

Programming Gateway HSM into an existing (Non-Gateway) nCipher security world

The Gateway allows use of an existing nCipher security world, including the use of any keys that were created using the "KeyStore.nCipher.sworld" keystore type, for the Gateway to use as the default keystore. Users would be required to manually program the security world on the nCipher HSM and populate it with their key data. When configuring the Gateway, users would then select the appropriate security world to use as the Gateway keystore.

Upgrading from Previous Versions

If the Gateway is being upgraded from a pre-6.0 version to the current version, a new HSM security feature, the keystore-protected master passphrase, will not initially be enabled. Users will have to disable the HSM, and then re-enable it. Once re-enabled, it will configure the Gateway to use a keystore-protected master passphrase.

Network Configuration

To achieve PCI DSS compliance, the server network must be properly designed.

The Gateway is highly configurable, and allows the user to enable and disable many different settings, startup parameters, and services on the appliance. In order to maintain compliance to PCI DSS, the following guidelines should be followed when configuring the Gateway.

Network Interface Configuration

The Gateway appliance comes with a built-in firewall and is designed to have network interfaces independent of each other, allowing for easy network segmentation. Ideally, the Gateway will straddle a network boundary, but it can also be deployed entirely within the DMZ. **For security reasons the Gateway should not be deployed fully outside the DMZ**.

The Gateway appliance is designed to make use of specific network interfaces for specific functions, in order to provide optimal security for the appliance itself.

eth0

The eth0 network interface is designed to be the primary “secure zone” interface. It is meant to be exposed to internal resources only and will allow connections on the following ports by default:

- 8080 – standard HTTP port
- 8443 – standard HTTPS port
- 9443 –HTTPS port without client certificate support
- 3306 – JDBC communication port
- 3307 – JDBC redirect port
- 2124 – Gateway inter-node communication port
- 7001:7100, UDP 8777 – JGroups communication for inter-node caches
- 22 – default SSH port

This network interface should never be exposed to the public internet, and should be protected by the firewall to be accessible only from internal sources. Port 8080 can

be closed if users wish to restrict access to secure access only, and port 22 can be closed if users wish to allow no SSH access to the Gateway appliance. If the Gateway is not in a clustered environment, the JGroups ports can also be disabled. All other ports must remain open in order for the Gateway to operate correctly.

eth1

The eth1 interface is designed to be the primary public-facing Ethernet connection. It is meant to receive incoming requests for the Gateway to process from either internal or external sources. As such, it is protected by the firewall, and only the following ports are open by default:

- 8080 – standard HTTP port
- 8443 – standard HTTPS port
- 9443 – HTTPS port without client certificate support

In order to maintain PCI DSS compliance, no other ports should be opened on eth1 unless specifically required by the Gateway to receive additional request traffic (FTP, SMTP). Further, the standard HTTPS port should be limited to message traffic only – see "Enabling a Specific Administration Port" below.

Additional network configuration

The Gateway comes with a total of four network interfaces, which can be enabled for various specific requirements, used as additional inbound traffic interfaces, or bonded with existing NIC's for greater bandwidth. Please contact CA support for assistance with configuring additional network interfaces.

All the ports that the Gateway appliance uses are configurable within the application, in terms of numbering, usage, and resourcing. To configure the ports, please see *the CA API Gateway Installation and Maintenance Manual* and the Policy Manager documentation. Because PCI DSS limits access to the box over secure connections only, users wishing to ensure PCI DSS compliance may want to disable port 8080 on eth1 and only allow SSL connections into the Gateway.

Other Configuration Considerations

Gateway Remote Access

In order to configure the Gateway, or modify the operating system parameters, the appliance must be accessed directly at the command line. The Gateway can be accessed via SSH (on the private Ethernet connection) or direct console access, and access rules can be modified. Depending on which method you choose to allow, users will want to consider the following guidelines:

SSH access on Private Network – internal access only

By default, the Gateway is configured to allow SSH access via the private network interface (eth0), using a single-factor authentication of username/password. If you wish to allow SSH, PCI DSS compliance is best achieved if eth0 is only accessible internally. This can be achieved by blocking external connections to eth0 on the Gateway at the company perimeter firewall.

SSH access on Private Network – external access

External access to eth0 is discouraged for security reasons; the Gateway should always have port 22 blocked from external access. If external SSH access to the Gateway must be granted, then a secondary jump server should be utilized between the external user and the Gateway, in order to provide two-factor authentication to the Gateway and fulfill PCI DSS compliance. The firewall would need to be configured to allow access to the jump server, where the user would logon with a set of credentials, and then SSH from there to the Gateway.

Direct console access

The Gateway can be configured only for direct console access by simply disabling SSH on all Ethernet ports. This can be done by disabling the SSH port (22) on all network interfaces via the Gateway firewall, or removing all users from the SSH "allowed users" list. In this scenario, a user would have to physically log in via a keyboard connected directly to the appliance.

Ensure NTP configured to use local time source

The Gateway makes use of the Network Time Protocol (NTP) in order to keep accurate time with other servers in its network. PCI DSS requires that time synchronization should be obtained from a single external source to a single internal source, and that all internal resources get their time from that internal source.

When configuring the Gateway, ensure that you select an internal server to use as the time source for NTP.

Account Management during Configuration

When configuring the Gateway using the configuration wizard, users will be asked to create special purpose users. Each of these users will require passwords to be set, but the configuration wizard will not enforce PCI-DSS password strength standards. Therefore, care must be taken to create a suitably strong password for these users.

SSM Admin user

The Policy Manager administrator account and password are not default users; they are set during the initial configuration of the CA API Gateway. However, passwords

for this user are not initially controlled by password rules, and can be set to any password that meets the minimum length. During configuration, the password must be set to something that is secure, or the password must be changed after logging into the Policy Manager for the first time.

In the event that the administrator user account needs to have its password reset (due to it being lost or forgotten), the reset script on the SSG that does this will reset that password to "password", and will not change it. In the event that the administrator password needs to be reset on the Gateway, the admin user must login to the Manager and change the password to a new value immediately.

Database Access Accounts

For database connectivity, the Gateway will require a credential for general read/write access to its database. The user ID and password are created during configuration, and users must ensure that the password is of sufficient strength.

Restrict Configuration Access to the Appliance

The Gateway comes with a configuration group named "ssgconfig". Any member of this group can log in to the Gateway at the console (or via SSH, if SSH is enabled), and access the Gateway configuration menu to configure the Gateway, start and stop the process, configure the HSM, and perform other related tasks.

Customers are able to create and add as many users as they like to the ssgconfig group. However in the interests of security, the list of people who are able to configure the Gateway should be kept to a minimum.

Chapter Four: Access Control and Gateway Management

Once installed and configured, the CA API Gateway is administered via the Policy Manager. The Policy Manager allows users to publish services, build policies, administer internal users and external LDAP repositories, and administer other related options.

In order to maintain PCI DSS compliance requirements around strong access control measures, the following guidelines should be followed for administering the Gateway.

Setting PCI DSS Defaults and Alerts

The CA API Gateway can be configured to adhere to almost all PCI DSS standards in its default setting. Additionally, there is a cluster property that when set, will clarify minimum strength requirements for passwords, maximum idle times for administrative sessions, and will provide additional audit records to indicate when the Gateway is configured to be below the PCI DSS standards. To enable this property, do the following:

1. Log in to the Policy Manager.
2. Navigate to **Tasks** > **Manage Cluster-wide Properties**.
3. Click [**Add**].
4. In the Key field, locate the key **security.pcidss.enabled**.
5. In the Value field, change the value from **false** to **true**.
6. Click [**OK**].

This cluster property will add warnings and audits for the following conditions:

- Password policy for the Gateway does not meet PCI DSS minimum standards.
- Administrative user account policy for the Gateway does not meet minimum standards.
- If the Gateway is using the audit sync policy and it fails, and the fallback to local database option is disabled, an audit will be logged in the local database indicating that the audit failed. This ensures that audits are never lost without alerting the user.

The cluster property should take effect after 15 seconds. Once set, both the password policy and administrative user account policy should be set to adhere to PCI DSS standards.

Access via the Policy Manager

The CA API Gateway Policy Manager is designed to connect to the Gateway via secure (HTTPS) connection, over the default port configured for SSL traffic during configuration. It supports either username/password or x509 certificate-based authentication, however it does not support two-factor authentication nor will it support authentication via a jump server. Therefore, connections to the Gateway via the Policy Manager should be limited to internal network access only, and attempts to administer the Gateway over the public network interface should be blocked at the perimeter firewall.

The private network interface is configured to allow administrative connections over SSL on port 8443.

Disabling Administration for Public-facing Ethernet

The Gateway comes with two pre-configured SSL-enabled ports on eth1, 8443 and 9443. Both are initially enabled for message traffic and administration; however, because public-facing network interfaces should not be used for administration purposes, it is strongly recommended that both be disabled for administration. Depending on message traffic needs, users may wish to disable one entirely, and only have a single SSL-protected inbound port. This can be done by doing the following:

1. Log in to the Policy Manager.
2. Navigate to **Tasks** > **Manage Listen Ports**.
3. Highlight one of the ports, click **Properties**.
4. On the right side of the properties dialog, in the Enabled Features section, clear the check boxes for [**Policy Manager access**] and [**Browser-based administration**].

Do the same for the other port. If users are deleting a port entirely, simply highlight the port and click [**Delete**].

In order to create a port for administration that is not available on the public-facing ethernet, users must create a new SSL-based port and bind it to the internal ethernet. For more information, see *Managing Listen Ports* in the Policy Manager documentation.

Keystore Configuration for the Gateway

The Gateway appliance comes with support for both software keystores and hardware (HSM) key management. In a PCI DSS configuration, it is strongly recommended that the HSM be used for key management, due to the secure nature of the key storage and inability for a single person to get access to the keystore.

Once the HSM is configured and being used for the keystore, the following recommendations should be followed:

- Create a private key for the securing of audit records. The purpose of this keystore will be to protect audited messages and details, in the case that cardholder data is being included as part of an audit record. This keystore will be used only for this purpose, thus ensuring that all audits are protected with a single purpose keystore.
- If a new security world and keystore were created during the Gateway configuration, then it will be required to create or import a CA key onto the HSM. The CA will be used for creating client certificates for users to authenticate with.

The Gateway will need to be restarted after creating a CA key in order for it to be picked up.

Password Management for Resources

Resources that are configured via the Policy Manager and which use credentials (for example, HTTP endpoints, JDBC connections, email listeners, LDAP providers, etc.) should have passwords configured beforehand in the Manage Stored Passwords task. This task ensures that passwords are not written in plaintext to the configuration database, but instead are referenced securely when configuring policies and entities.

For more information, see *Managing Store Passwords* in the Policy Manager documentation.

Configuring Inbound and Outbound Security

PCI DSS compliance requires that all inbound and outbound connections from a network device use strong encryption. The Gateway provides for automatic encryption of all administration functions, and provides the means necessary to encrypt message traffic both inbound and outbound. The following needs to be done to ensure that your transport level encryption is strong enough to satisfy PCI DSS standards.

SSL Requirements for Message Traffic and Administration

Ports configured for HTTPS communication are automatically configured to accept incoming connections only using TLS 1.0. TLS 1.1 and 1.2 can be optionally selected as well. The Gateway does not accept SSLv2 incoming connections by default, except in the case of an SSLv2Hello.

The Policy Manager provides the ability to override accepted protocols (to allow SSL v3), or force the Gateway to not accept "SSLv2Hello". To do this:

1. Log in to the Policy Manager.
2. Navigate to **Tasks** > **Manage Listen Ports**.
3. Highlight the port you wish to configure, click **Properties**.
4. Click the [Advanced] tab.
5. In the [Advance Properties] tab, click [**Add**].

In order to allow SSLv3, enter the following for property name and value:

- Property Name: **overrideProtocols**
- Property Value: **SSLv3**,[others that would be required, TLSv1, TLSv1.1, TLSv1.2, comma separated]
    - If you wish to disallow SSLv2Hello, leave it out of the property value

In order to disable SSLv2Hello only, enter the following property:

- Property Name: **noSSLv2Hello**
- Property Value: **true**

In a PCI DSS complaint system, SSLv2 or lower should never be allowed for message level communication or administration.

SSL Configuration for Outbound Connections

Configuration for secure connections from the Gateway to backend services can be done on a per-policy or per-endpoint basis. There is currently no way to globally enforce SSL connectivity outbound from the Gateway.

Configuring for an endpoint

The "Manage HTTP Options" dialog allows users to setup specific HTTP and HTTPS rules for a common endpoint. In this dialog, users can describe protocols, specific keys, and a list of acceptable ciphers for a given endpoint.

1. Log in to the Policy Manager.
2. Navigate to **Tasks** > **Manage HTTP Options**.

3. Click [**Add**].
4. Fill in information for HTTPS cipers, protocols.

For more information, see *Managing HTTP Options* in the Policy Manager documentation.

If the HTTP endpoint requires credentials, the password must first be configured in Manage Stored Passwords:

1. Select **Tasks** > **Manage Stored Passwords**.
2. Create a password and indicate that it will be referenced as a context variable.
3. Navigate to **Tasks** > **Manage HTTP Options**.
4. Edit the HTTP endpoint created.
5. Fill in the username, and select the password that was created previously.

Once filled in, the Gateway will use these rules for all requests sent to the endpoint described, regardless of what policy sends to the endpoint.

Configuring in a policy

The Gateway allows users similar functionality on a policy-by-policy basis. The same SSL controls that you can set in "Manage HTTP Options" also appear in the HTTP routing assertion, under the security tab. Configuring the connection settings here will ensure that any requests that are sent to the particular policy will be routed to the backend using the SSL options set within the policy.

The Route via HTTPS assertion also allows the use of stored passwords in the password field, which are referenced using the format *${secpass.<passwordname>.plaintext}*.

Use of Internal Users for Gateway Administration

The Gateway comes with an internal identity provider (IIP), and the IIP should be used to house users for internal management of the Gateway. Unlike with external LDAP systems, the Gateway provides mechanisms to expire or disable users and enforce PCI DSS compliant password strength and password rules for those users.

Internal Users for Administration

It is required that in PCI DSS compliant instances, IIP users only be used for management of the Gateway. The Gateway does allow users from external LDAP repositories to manage the Gateway via the Policy Manager, however does not enforce any rules on the usernames or passwords.

If internal users are used for administration purposes, it is also recommended that they are not also used for authenticating message level traffic.

Setting the Internal User Password Policy

The Gateway comes with a password policy specific to PCI DSS password rules regarding strength, composition, and password expiry and reuse. If the PCI DSS cluster property is enabled on the Gateway, the Password Policy dialog will warn users when the password policy does not meet PCI DSS security standards, and an audit will be logged indicating that the password policy is not of sufficient strength.

Users can set the password policy automatically to the minimum PCI-DSS specified strength by clicking [**Reset to PCI-DSS Minimum**] in the Internal Identity Provider Password Policy dialog. The minimum password configuration looks like this:

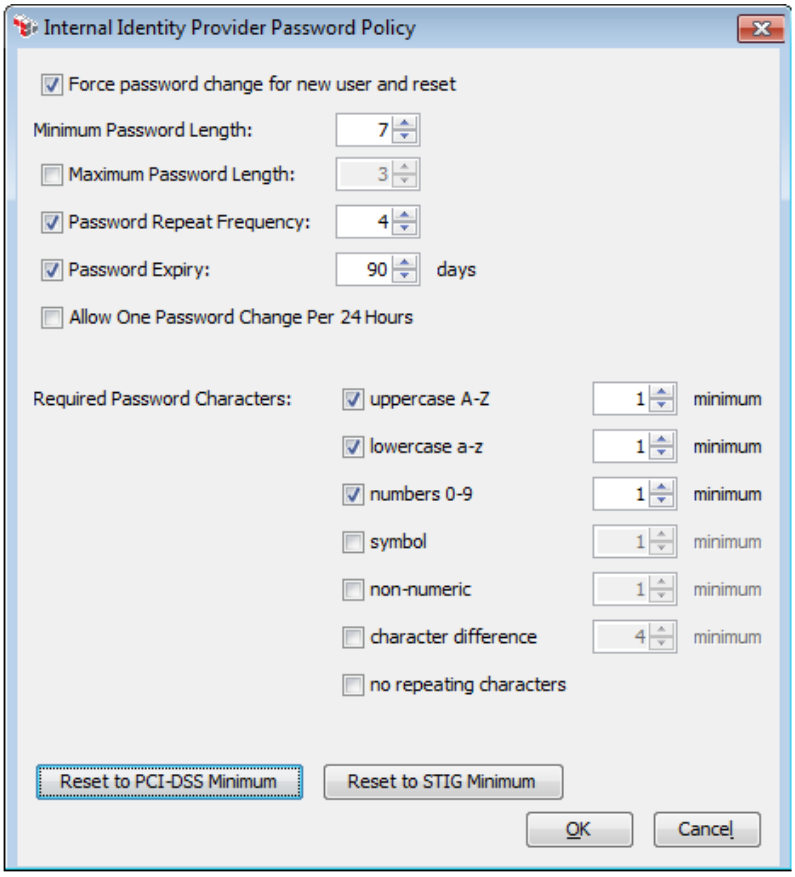

Figure 2: Internal Identity Provider Password Policy

If the PCI DSS security setting is not enabled, users can still enable a password policy that is PCI DSS compliant; however, no warnings will be given if that policy is below PCI-DSS requirements.

Administrators will be able to set or reset passwords with relaxed rules; however if a PCI-DSS compliant password policy is configured, an administrative user will be forced to change their password on next login.

Administrative User Account Policy

Administrative users (users that belong to the administrator role) are subject to additional rules around password expiry and account inactivity, due to the nature of the administrator role:

- While administrative users can have their passwords expire, the administrator role must have at least one user with a password that never expires. This is to prevent all administrative users from being locked out of the Gateway, and unable to administer. It is strongly recommended that administrative users be created with no password expiry. If you wish to create users that do have administrative account password expiry, you must ensure that one administrative user does not have an expiry on their password. The Gateway will ensure that at least one user does not expire.
- Administrative role users are exempt from account inactivity. Even if the password policy dictates the inactivity time (number of days of non-use before the account is disabled), if the user belongs to the administrative role, that account will never expire. Therefore, it is important to remember to manually disable administrative accounts if the account is no longer needed.

Disable HTTP Digest to Prevent use of MD5 Algorithm

The Gateway provides support for HTTP Digest authentication, which requires passwords to be stored in HA1 format, and the MD5 algorithm to be used for password verification. However, MD5 is not a suitably strong hash for PCI DSS security considerations, and should not be used when storing passwords in the Gateway user database.

To avoid storing HA1 passwords, HTTP Digest is now disabled by default in the Gateway, via the cluster property “httpDigest.enable”. As long as digest authentication is set to false, passwords will only be saved using the new stronger SHA512Crypt algorithm, which is suitably strong for PCI DSS storage requirements. If HTTP Digest is enabled passwords will be stored in both SHA512Crypt and HA1 formats. Therefore, **PCI DSS installations must ensure that HTTP Digest is disabled in the Gateway product**.

Upgrading Internal Users from Previous Versions

If a Gateway is being upgraded from a pre-6.0 version to 6.0, the IIP will contain passwords stored in HA1 format. Therefore, in order to maintain PCI DSS compliance, and not have any passwords stored in HA1 format, the administrator should invoke the “Force password change for new user and reset” option in the Internal Identity Provider Password Policy dialog in the Policy Manager.

For more information, see *Managing Password Policy* in the Policy Manager documentation.

Audit System Guidelines

The Gateway comes with an auditing system that provides an audit trail for system, administrative, and optionally message level traffic. In order to maintain PCI DSS compliance, the following rules should be adhered to.

Administrative Audit System Settings

In order to maintain PCI DSS compliance, the Gateway should be allowed to log all system and administrative events, and should not be in a situation where audits are not logged or fail to log for any situation. Therefore, the *audit.adminThreshold* cluster property should be set to INFO, which is the level that most administrative audits are set at.

If the value for this cluster property is higher than INFO, many administrative audits will not be audited, resulting in an incomplete audit record.

Storing Message Audits in the Gateway Database

If you are using the Gateway database to store audit records, it is strongly recommended that the Audit message Filter (AMF) and Audit View Policy (AV) are used to protect and limit the viewing of sensitive data.

Exposed as internal services, the AMF allows a copy of the message to be processed for the purposes of auditing the message in a PCI DSS compliant fashion. The AMF policy should be constructed in such a way that sensitive authentication data that cannot be stored is removed from incoming messages, and cardholder data that can be stored is encrypted for storage. This allows users to seamlessly audit messages in a PCI DSS compliant manner as part of the request processing.

The AV Policy is another internal service which will have a policy that works in conjunction with the AMF policy, and allows messages that were encrypted or altered with the AMF to be rendered correctly for the purposes of viewing them.

See the Policy Manager documentation for further information on publishing and using the AMF and AV Policy for protection of audit data.

Separate Key for Protecting Audit Records

The AMF policy allows users to optionally protect request or response messages that are included as part of an audit record. If the AMF is being used for this, it is recommended that a separate key is created for this purpose. The AMF would use

the public key to encrypt audit record details, while the AV Policy would use the private key to decrypt the same messages when viewing them. Using a separate key, that is only used for this purpose, ensures that encrypted data cannot be accidentally decrypted easily.

If not done already, users should create a new private key, and designate that key to be the "AV" key, used for the AV Policy to decrypt audits.

When configuring the AMF policy, any assertions that are used to encrypt XML elements should be configured to use the public certificate of the AV key to encrypt. When users use the AV Policy to view encrypted audits, they will then be decrypted.

See the Policy Manager documentation on configuring and use of the Audit Viewer Private Key for more details.

Using Offbox Audits

The Gateway comes with a default Internal Audit Sink Policy configured. This policy is configured to fail by default, therefore it must be updated. When constructing a policy, follow the following guidelines:

- Keep assertions to a minimum – message manipulation and transformation not related to auditing should be done within the main service policy.
- Ensure that the offbox audit location is reachable – the offbox audit policy will attempt to send audit records to another location, it is important to ensure that the endpoint is reachable.
- Use an SSL-protected endpoint – in order to ensure compliance with PCI DSS, audits sent to an offbox location should be sent using secure communication.
- Use encryption assertions to encrypt sensitive parts of the message.

In the event that the offbox audit policy fails, the Gateway has a fallback setting, whereby any audits that cannot be sent offbox can instead be saved to the internal database. The cluster property audit.sync.fallbackToInternal is set to true by default. In order to ensure that no audit records are lost, this setting should not be altered.

For more information, see Working with the Audit Sink Policy in the Policy Manager documentation.

Role-Based Access (RBAC) Guidelines

The Gateway utilizes a Role-Based Access (RBAC) system for assigning roles to individual users. Some roles are present by default on an Gateway when first starting up, others are created to manage new entities (services, LDAP repositories, UDDI's) as they are published or made known to the Gateway.

PCI DSS has specific rules around compartmentalizing access to cardholder data, or systems that have cardholder data going through them. In order to remain compliant, the following rules around administrator and audit roles must be followed.

For more information, see *Managing Roles* and *Predefined Roles and Permissions* in the Policy Manager documentation.

Administrator Role

The administrator role allows users to administer all aspects of the Gateway, via the Policy Manager. Users added to this role will be able to administer all aspects and functionality in the SSG, with the exception of invoking an Audit Viewer Policy. Administrators do have the ability to assign users to the Invoke Audit Viewer role, and are the only role that has that ability.

Due to the power that the administrator role has within the Policy Manager, it is recommended that users that have administrator role do not also give themselves Invoke Audit Viewer role, but rather have distinct users for both roles.

It is recommended that customers keep the number of administrative users to a minimum, as dictated by their business needs.

Invoke Audit Viewer Role

The Gateway provides a new role that enables members to view audit records protected by an Audit Message Filter (AMF) policy. This role is not granted to any user by default, and only an administrator can grant this role to other users.

In a PCI DSS compliant deployment, the Gateway should use the AMF policy to protect cardholder data in audit records. If users are using the AMF policy to protect cardholder data in audit records, the Invoke Audit Viewer roles will allow users to view protected audit data. This role should only be granted to individuals who have a business need to view this data.

View Audit Role

The View Audit role allows users to view audits, but does not allow the AV Policy to be applied to protected audit records. Audits containing no protected data will be shown in clear text, while any protected audit records will be displayed in their protected format.

Login Expiry

The Policy Manager has two timeout features that users should be aware of:

Gateway Session Expiry

The Gateway Session Expiry is controlled through the Administrative User Account Policy and defaults to 30 minutes. After 30 minutes of inactivity, the logged-in user must re-authenticate their credentials to continue using the Policy Manager.

If the Gateway is configured to be PCI DSS compliant, the Administrative User Account properties will display a warning if this value is greater than 15 minutes, indicating that it is beyond the PCI DSS minimum value. Users must change the session expiry to 15 minutes in a PCI DSS compliant environment.

For more information, see *Managing Administrative User Account Policy* in the Policy Manager documentation.

Policy Manager Inactivity Timeout

The Manager Inactivity Timeout is set in the Preferences in the Policy Manager, and defaults to 30 minutes. The Gateway session expiry value overrules the inactivity timeout, therefore the Manager will become inactive if the Gateway session expires.

For more information, see *Configuring Preference*s in the Policy Manager documentation.

Chapter Five: Policy Construction and Assertion Usage

The Gateway policy assertions allow users to build security policies, in order to protect backend resources. They allow users to make decisions based on message content, authentication success or failure, and other parameters, and route messages accordingly.

Policies that will handle cardholder data should be constructed with the following.

Securing Inbound/Outbound Traffic

All inbound and outbound traffic through the Gateway that contains cardholder data should be secured.

Any policy that is created, that accepts incoming HTTP requests from outside the Gateway, should be configured with the “Require SSL/TLS” assertion. This will force the Gateway to only accept requests via SSL. The SSL assertion has an optional requirement for a client certificate, which can be used to provide mutual authentication.

If the Gateway is accepting requests over a queue (via JMS), then the queue provider should be configured to use SSL.

All policies that send data out from the Gateway to another endpoint should use secure transport protocols. This includes routing assertions (HTTPS, FTPS, JMS over SSL) or offbox audits (sent over HTTPS only).

Some assertions allow policies to obtain resources from external sources (Validate XML Schema, XSL Transformation, Create XACML Request). If these assertions are configured to get their resources from an external source, and continually monitor that source for updates, then the URL that is monitored should be an HTTPS endpoint.

Removing Sensitive Data for Auditing

If a policy is using auditing functionality, where the request or response message is saved as part of the audit trail, then the copy of the message that is audited must have certain cardholder data elements removed before adding it to the audit record. PCI DSS specifies what parts of cardholder data must be removed from a message and what parts must be obfuscated. The Gateway provides assertions that allow

users to alter the content of a message, and an internal policy that will specifically do this for the purposes of auditing.

Audit Message Filter Internal Policy

The Audit Message Filter (AMF) policy is designed to filter request and response messages, if they are going to be included in the audit trail for a particular transaction. The AMF policy can use any of the Gateway assertions to modify the message as required by your organization. The modified version of the message will then be stored in the Gateway database.

In order to ensure that messages being audited contain no cardholder data, the AMF Policy should be utilized for all auditing for policies that will handle sensitive data. Please see the Policy Manager documentation for further information regarding the AMF Internal Policy.

AMF Internal Policy Construction

Assertions that are available to regular service policies are also available inside the AMF policy, and these assertions should be used to remove sensitive cardholder data from messages, before they are audited.

If an incoming message contains cardholder data, the following modifications must be made to the message before storage:

- Magnetic strip, card validation code, and PIN data must be fully removed from the message
- The Primary Account Number (PAN) should be encrypted using strong encryption
- Cardholder name, service code, and expiration date can optionally be encrypted (as long as the PAN is encrypted this data does not absolutely need to be encrypted).

The following assertions will be useful in the modification of the message:

XSL Transformation Assertion

If the incoming message is XML, the XSL Transformation assertion can be used to strip cardholder data from the message entirely, or replace the contents of the elements with other data. This assertion uses the XSL language to manipulate the contents of XML messages, and relies on the author understanding the structure of the XML message being modified.

Evaluate Regular Expression Assertion

The Evaluate Regular Expression assertion can be used on both XML and non-XML messages to replace data based on a regular expression pattern. This

method can be used to replace the CCN with other characters, or to remove the contents of entire elements from a message

XML Encryption

XML encryption assertions allow the data to be preserved, but protected while persisted to disk by encrypting the contents.

Add or Remove XML Element(s)

This assertion allows users to remove elements from messages, based on assignment of elements to variables. This method can be used to remove cardholder data from standard XML messages.

It is expected that users will employ more than one assertion in the AMF policy to properly ensure that audited messages adhere to PCI DSS standards. A sample AMF policy used to make auditing requests PCI DSS compliant might look like this:

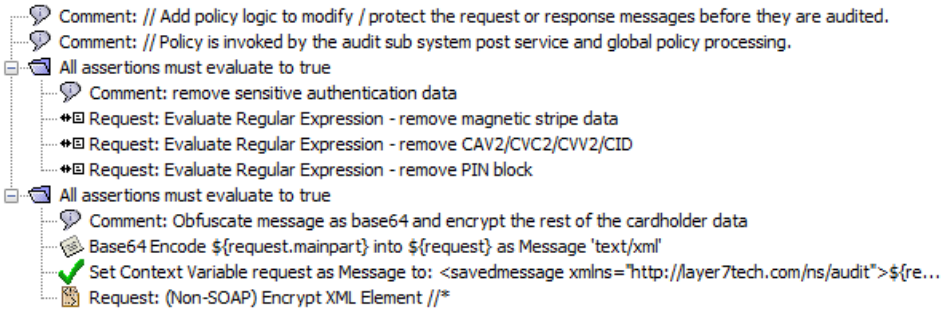

Figure 3: Sample AMF Policy

In this policy, the request message sent to the Audit Message Filter policy has any sensitive authentication data removed via regular expression pattern matching. The rest of the message is then converted to base64 and XML, and then encrypted to protect the rest of the cardholder data.

Use of Context Variables in Policy

The Gateway both sets and allows the setting of several context variables within a service policy. Some variables are set automatically, others can be set within assertions, and many assertions can use those variables to make policy decisions, capture values from messages or fragments of messages themselves.

The following context variables should be used with caution in general:

- <request>.mainpart
- <request>.parts.body
- <request>.originalmainpart
- Audit.var.<origvar>, where “origvar” is one of the message variables

- Audit.request
- Audit.response

While it is expected that the above assertions may be used for making policy decisions, they should not be used in any assertions that are capable of persisting data to disk, or sending data out of the Gateway in an unintended manner. The following assertions should avoid the use of any message variables:

- Send email alert: this assertion is designed to send information off of the Gateway in the contents of an email. The use of message variables in this assertion may cause the cardholder data to be sent to an outside location.
- Template response: this assertion will send back whatever is in the message section to the requestor, as a response.
- Add Audit Details: this assertion will create a record as part of the audit trail for a message, with customized information in it. However, unlike regular audits, the audit details assertion will not be subject to the AMF policy to remove sensitive data. If the Audit Details assertion uses a message variable, message variables should not be included as part of the detail message.
- SNMP Trap: this assertion will instruct the SSG to broadcast an SNMP trap to a predefined network address. The text field allows for the use of context variables, which could contain cardholder data.

Other assertions are able to capture parts of a message, and save those parts as variables (to be used later). The following assertions should be used to manipulate and store data carefully:

- Evaluate Request XPath
- Evaluate Response XPath
- Apply XSL Transformation
- Evaluate Regular Expression :

These four assertions are able to extract information out of a message – either element values or entire XML fragments - and save them into other fragments.

In order to maintain PCI DSS compliance within the Gateway, it is strongly recommended that users do not use the above variables to access parts of any message that may contain unencrypted cardholder data,

Use of Passwords in Assertions

Many assertions in the Gateway allow users to add credentials to the assertion, in order to access protected resources (FTP routing, email alert assertion, etc). If credentials are stored in policy assertions in plaintext, then they are also saved to the Gateway database in plaintext, as part of the policy XML.

PCI-DSS requires that passwords are never stored in clear text in a configuration file or database. In order to avoid plaintext passwords being present in the database, users should use the "Manage Stored Passwords" functionality present in the Gateway. Accessed via the Policy Manager, this utility allows you to store passwords in encrypted format, and then reference the password as a context variable in policy assertions as required.

See the Policy Manager documentation for further information on this functionality.

HTTP Digest Authentication

Although the HTTP Digest assertion can be used with the Gateway, users who are in PCI DSS-aware environments must refrain from using this assertion. The HTTP Digest uses the MD5 algorithm for password verification, as specified by the HTTP Digest specification, but this is not a strong enough algorithm to be considered PCI DSS compliant.

Building Secure Policies

The Policy Manager policy builder allows users to create service policies that help to protect against threats and limit the information that is passed back to users.

Avoid Anonymous Policies

To ensure that only authorized people have access to consume a Gateway service and Gateway endpoint discovery via the WSIL (Web Services Inspection Language) viewer, each service should require some form of credential authentication; otherwise, anonymous consumption will be possible and anonymous endpoint discover may be possible.

When a SOAP service is published for the first time and saved, it is made active with only a routing assertion and no requirement for user authentication. This means that it can be consumed by any user sending a request to the Gateway.

When publishing SOAP-based services, it is recommended that users immediately protect the service by requiring credentials to consume it. If a credential mechanism has not yet been decided upon, the service should be disabled until it is ready to be published.

Threat Protection

The Gateway protects against many threats inherently, and also has assertions that provide additional threat protection to be added to service policies. When constructing policies, the following threat protection assertions should be considered, in order to comply with PCI DSS protection:

Protect Against Cross-Site Request Forgery

This assertion helps to protect against cross-site request forgery

Protect Against Code Injection

This assertion will help protect against many different injection attacks, including code, LDAP, and XPATH injections

Protect Against Message Replay

This assertion will help protect against a replay attack, whereby the same message is sent twice. This protection is cluster-wide, so malicious users cannot attempt to send the same copy of a message to 2 different nodes within the same cluster.

Protect Against SQL Attack

This assertion helps to protect against various SQL injection attack profiles. Policies can protect against attack parameters for specific database products, or can globally protect against them all.

Customized Error or SOAP fault Response

The CA API Gateway has a built-in error handling process, and will return faults to the user when policies are violated or resources otherwise cannot be reached. However, if users wish to limit or customize the information sent back to the user in error situations, or remove error responses entirely, the Customize Error Response or Customize SOAP Fault Response assertions can be used in policy. These assertions allow customized responses to be sent as errors, with as much or as little information as is deemed necessary. The assertions also give the ability to drop error connections entirely.

Chapter Six:
CA API Gateway Maintenance

All components of the CA API Management can be updated using the CA API Gateway main menu. The Gateway has a built-in update facility that allows it to recognize and install CA update packages. The packages are built by CA, and are signed to ensure validity. For more information see *Managing Gateway Patches* in the *CA API Gateway Installation and Maintenance Manual*.

CA issues update packages for both operating system updates and Gateway product updates.

Operating System Updates

Operating system updates are issued once a month by CA, and will contain any updates to OS-level packages, or any security updates to packages. The OS updates can be downloaded from the CA website when they are completed.

CA API Gateway Updates

The CA API Gateway is updated from release to release (or with service pack patches) using the same CA patching system. These patches are released independently of OS level patches, but are applied in the same fashion.

Appendix A: CA API Gateway Services

The following is a list of the services that appear on the CA API Gateway, with their "as shipped" statuses.

Service	Default status	Reason for being enabled	Disable?
acpid	on	hardware power management system	no
anacron	on	command scheduling system	no (anacron is subtly different from cron,but should not be disabled either)
atd	off		
auditd	off		
autofs	off		
avahi-daemon	off		
avahi-dnsconfd	off		
cpuspeed	off		
crond	on	command scheduling system	no (raid status is monitored via a cron task)
cups	off		
exim	off		
firstboot	off		
gpm	off		
haldaemon	off		
ip6tables	on	system firewall for IPv6	yes (if not using ipv6)
ipmi	on	hardware management system	No (turning this off will mean that the ILOM or other similar devices cannot be used to monitor the system. The ESM also uses IPMI for some of it's monitors)
iptables	on	system firewall	no (SSG requires)

Service	Default status	Reason for being enabled	Disable?
irda	off		
irqbalance	on	rebalancing system for multiple processors	no (this will impact system performance and stability. This service does not have any network facing component.)
iscsi	off		
iscsid	off		
kdump	off		
krb524	off		
kudzu	off		
lm_sensors	off		
lvm2-monitor	off		
mcstrans	off		
mdmonitor	off		
mdmpd	off		
messagebus	off		
microcode_ctl	off		
multipathd	off		
mysql	on	SSG configuration database	no
netconsole	off		
netfs	off		
netplugd	off		
network	on	Operating system networking service	no
nfs	off		
nfslock	off		
nscd	off		

Service	Default status	Reason for being enabled	Disable?
ntpd	on	Operating system time synchronization utility	no
portmap	off		
psacct	off		
radiusd	off		
rawdevices	off		
rdisc	off		
readahead_early	off		
readahead_later	off		
restorecond	off		
rpcgssd	off		
rpcidmapd	off		
rpcsvcgssd	off		
rsyslog	on	syslog service	no (turning this off will mean that command line auditing and all system activity will NOT be logged to syslog [or external log sinks])
saslauthd	off		
smartd	off		
snmpd	off		
snmptrapd	off		
ssem	off		
ssg	on	SSG process	no
ssg-dbstatus	on	SSG process to control restarts in replicated environments	no
ssgsysconfig	on	SSG configuration utility	no
sshd	on	remote management service (ssh)	yes (if blocking ssh access)

Service	Default status	Reason for being enabled	Disable?
tarari	on	SSG management service for XML acceleration device	no
tcp_tune	on	SSG operating system configuration	no
xfs	off		

Index