Websense Content Gateway HTTPS Configuration

Support Webinars

web security | data security | email security

Webinar Presenter

Scott Peckenpaugh

- Title: Sr. Tech Support Specialist
  - Cisco Certified Security Professional
  - Microsoft Certified Systems Engineer

Goals and Objectives

- SSL Overview
  - General SSL information
- HTTPS Module Overview
  - WCG's HTTPS
- HTTPS Configuration
  - Configuration Steps
- SSL Bypass
  - Incident management
- Certificate Management
  - Managing Digital Certificates

SSL Overview

What is SSL?

- Secure Sockets Layer (SSL)
  - Provides security between server and client
  - Authenticates with a digital certificate
  - Encrypts using Public/Private key
  - Host side integrated into your web browser

Important elements of SSL

- Authentication
  - A digital certificate is tied to a specific domain
  - Issued by Certification Authority (CA)
  - The CA is a trusted third party
  - Confirms identity of the owner of the domain
  - VeriSign or Thawte

Important elements of SSL

websense
ESSENTIAL INFORMATION PROTECTION™

- Encryption
  - The process of transforming information to make it unintelligible to all but the intended recipient.
  - This forms the basis of data integrity and privacy necessary for e-commerce.
  - Uses the public-and-private key encryption system developed by RSA.

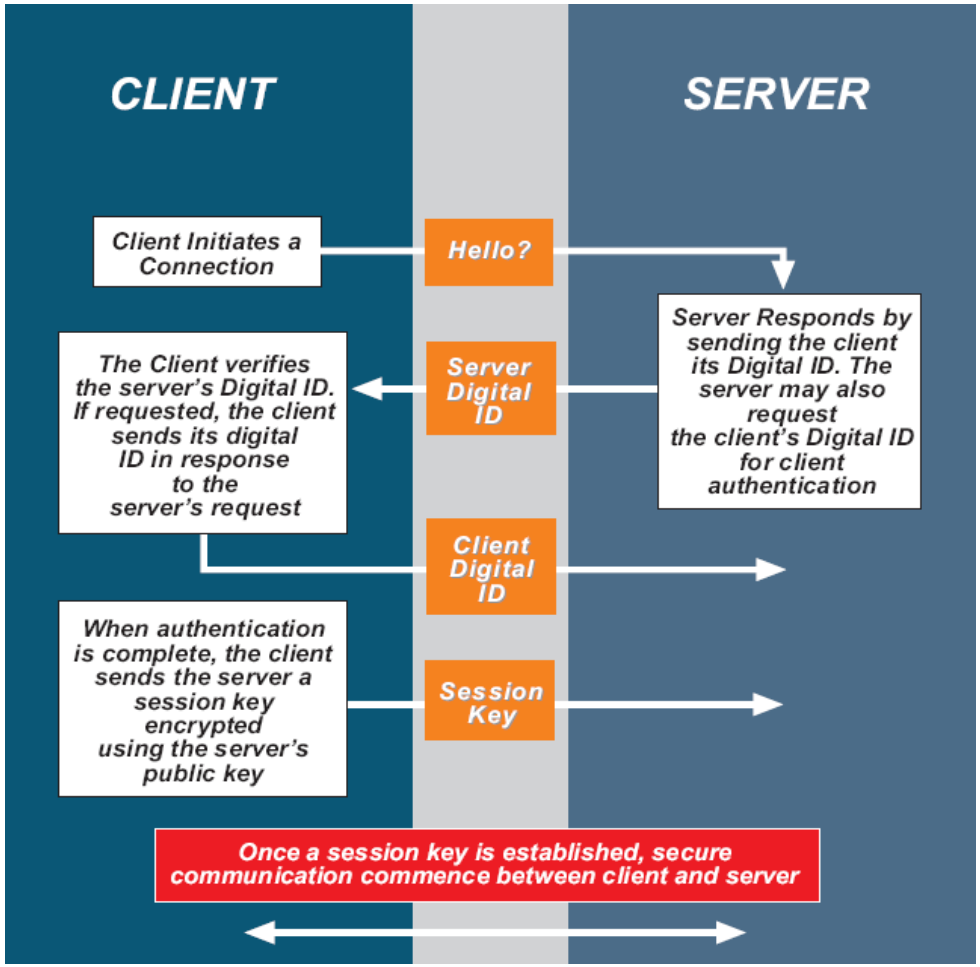
Public and Private Key

- Public Key
  - Numeric code used to encrypt messages sent to the holder of the corresponding private key.
  - Public key may be freely circulated without compromising encryption.

- Private Key
  - Numeric code used to decrypt messages encrypted with a unique corresponding public key.
  - Integrity of encryption depends on the private key being kept secret.

How is a SSL Session Setup?

- Client requests connection (lists supported Ciphers).
- Server chooses strongest mutual Cipher and sends Digital Certificate (DC).
- Client validates DC, encrypts a random number with Public Key.
- Server decrypts with Private key to get the random number.
- This shared secret random number is then used to encrypt all traffic.

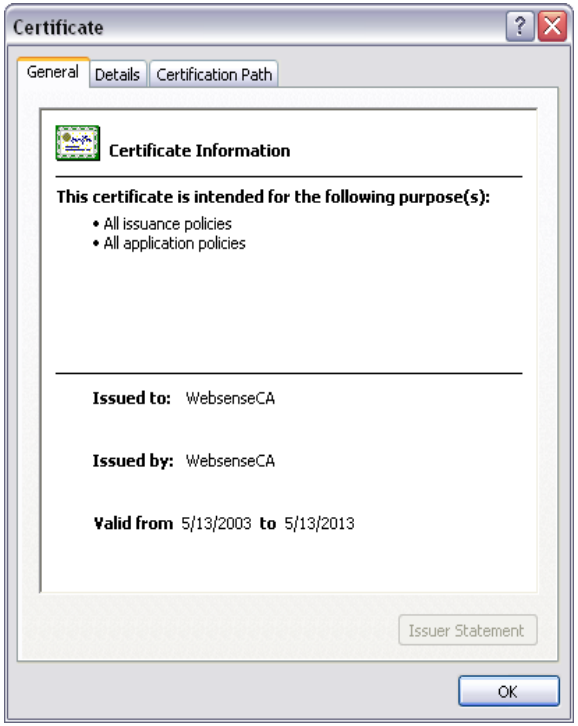


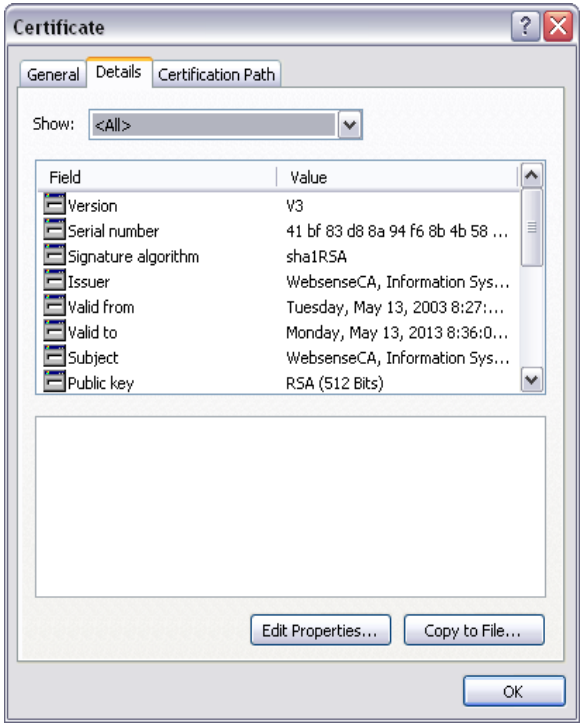
How to Tell if a Site is Secure

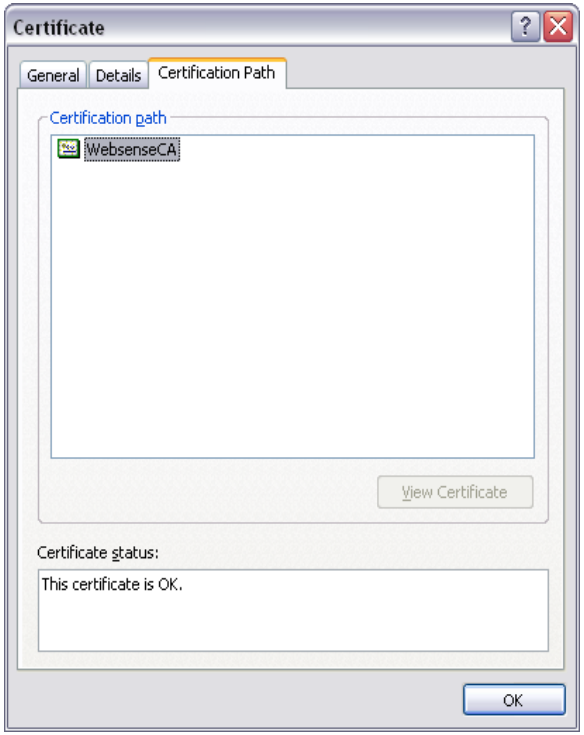
- Padlock
  - Look for a padlock on the browser status bar.
  - When a SSL session is established the padlock icon will appear.
  - The strength of the encryption can be shown by mouseing over the padlock on IE.

SSL Certificate

Internet Explorer







SSL Certificate

- The domain for which the certificate was issued.
- The CA which issued the certificate.
- Time period the certificate is valid.
- The owner of the certificate.
- The physical location of the owner.
- Certification path or Certificate chain

Issues with Certificates

- Certificates can be stolen, bogus, expired or revoked.
- The user, not the security officer, makes the final decision about the “trustworthiness” of a website or entity.
- In the best case, digital certificates can only guarantee the identity of a person or entity. They cannot provide any assurance about the person‘s intentions.

SSL Summary

- Secures communication between server and client.
- Authenticates with Digital Certificate
- Encrypts with Public/Private keys
- CA's are trusted 3rd party

HTTPS Module Overview

SCIP

- Websense has contracted with Microdasys to provide the HTTPS termination process used by WCG.
- SCIP - Secure Content Inspection Proxy
- SCIP provides 2 primary areas of functionality:
  - Certificate Validation
  - Proxy

Certificate Validation

- Certificate Validation
  - Digital certificates are checked for validity.
  - SCIP catches bogus, self-signed and revoked certificates
  - Certificates are inspected and allowed or denied at the gateway level, based on security policies, not the discretion of the client user.
  - Automatic revocation checking with Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) support.
  - Extensive exception handling and incident management capabilities.

Proxy

- Proxy
  - The data is decrypted, forwarded to WCG.
  - WCG applies inspection rules (ie. WSE, Analytics)
  - Re-encrypted and sent to its destination.
  - Applies security policies to all encrypted inbound and outbound Internet traffic.
  - Data can be decrypted and hence inspected for malware.

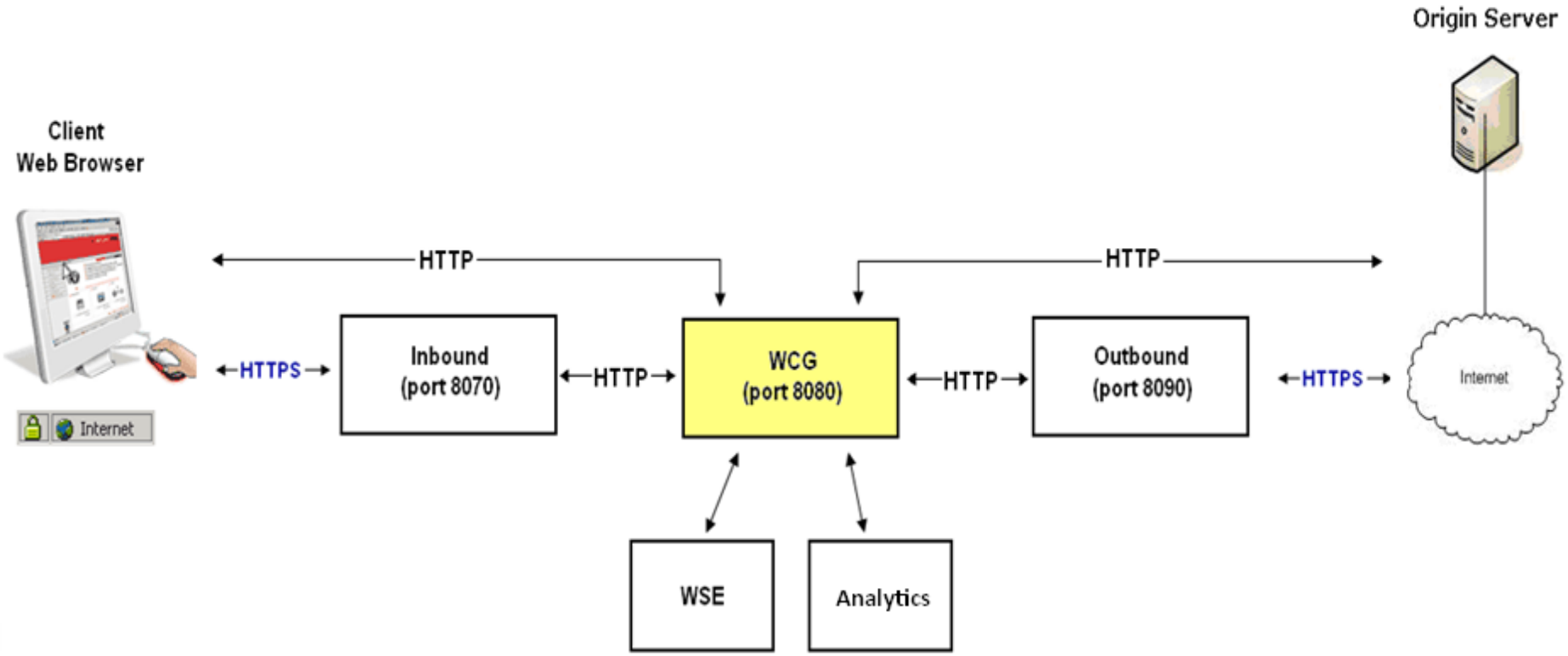
SCIP

- Certificate validation ensures the following
  - Certificate is not revoked
  - Certificate is not expired
  - Certificate owner and URL have the same identity
  - Certificate is issued by a trustworthy CA
- Network Security Administrator has the power to decide which site to be allowed not the client.
  - Any decision about the trustworthiness of a certificate must be made solely by the security administrator.
  - Any exception to the rule can only be made and allowed by the security administrator.
  - The user of a client workstation can only request exceptions, but not make them.
- Control over data transmitted
  - Data can be decrypted and hence inspected for malware.

Traffic Flow

The client will accept the certificate without prompting the user if the following three requirements are fulfilled:

1 The certificate is signed by a trusted CA
2 The certificate is valid
3 The URL matches the Common Name Field of the Certificate.



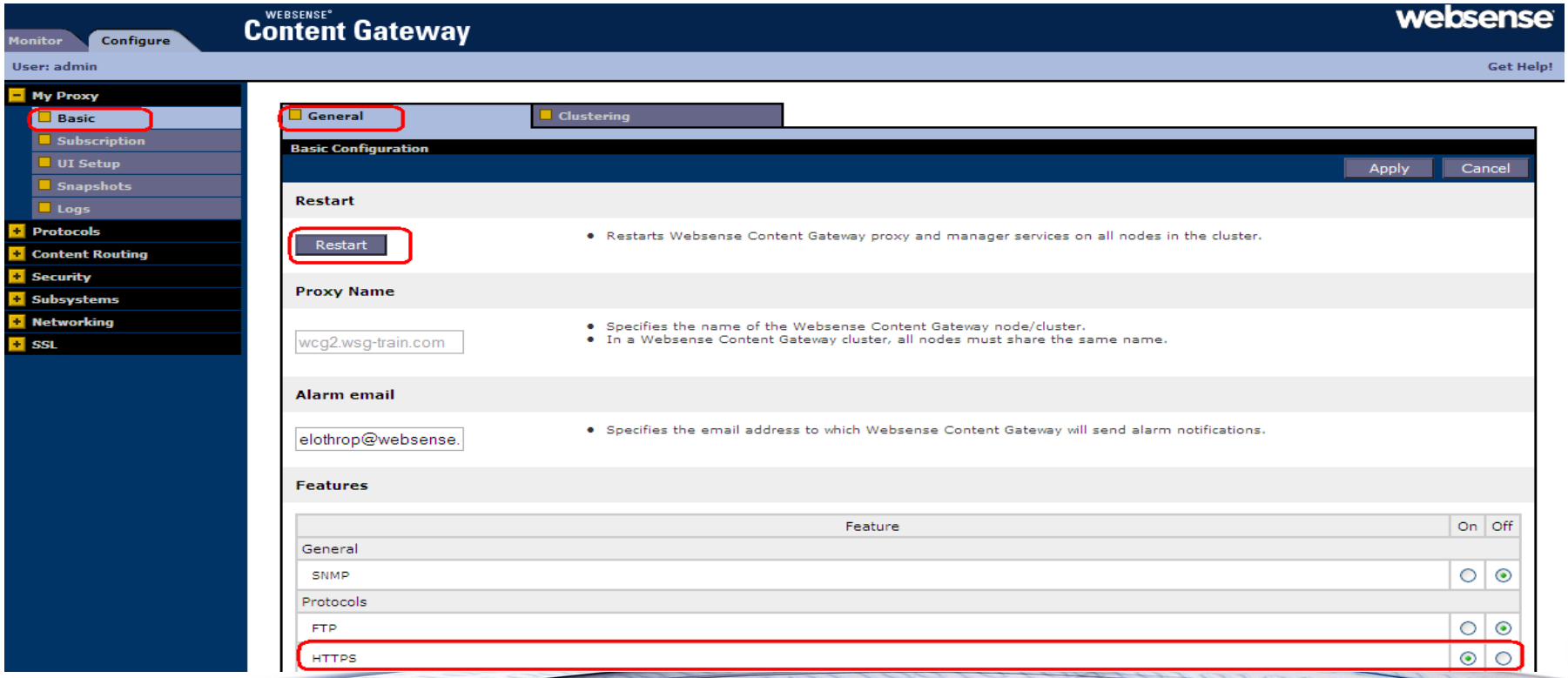
HTTPS Summary

- SCIP
  - Secure Content Inspection Proxy
- Certificate Validation
  - Common Name, Date, CA
- Proxy
  - Allows inspection of packet

HTTPS Configuration

SSL Decryption

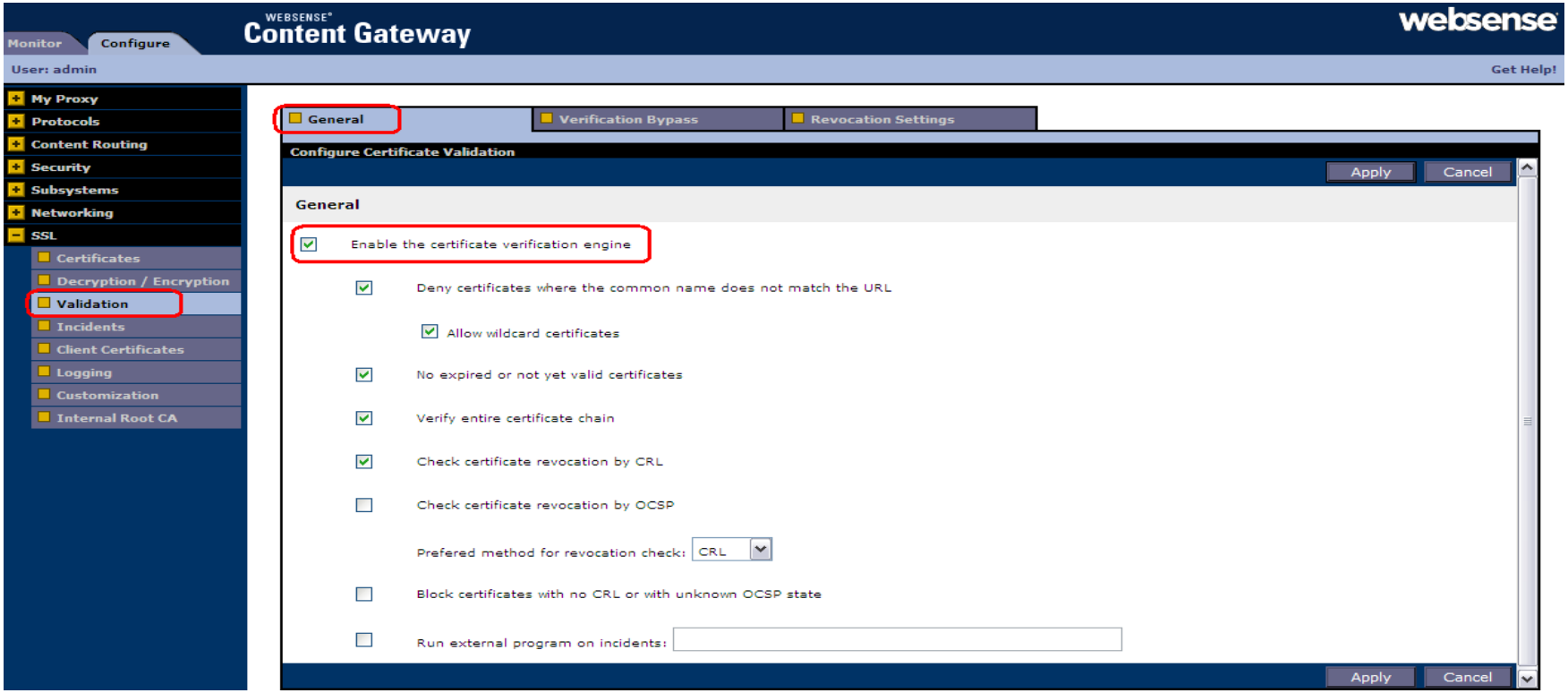
- To enable the SSL configuration options, you first need to enable the SSL Decryption Feature.
- Configure > My Proxy > Basic > General > HTTPS
  - Select “On” Radio Button
  - Click Apply
- Configure > My Proxy > Basic > General > Reset
  - Click Restart



Certificate Validation

Enable the Certificate Verification Engine

- To enable or disable verifying certificates and checking for certificate revocation.
- If this option is not selected, checking does not occur.



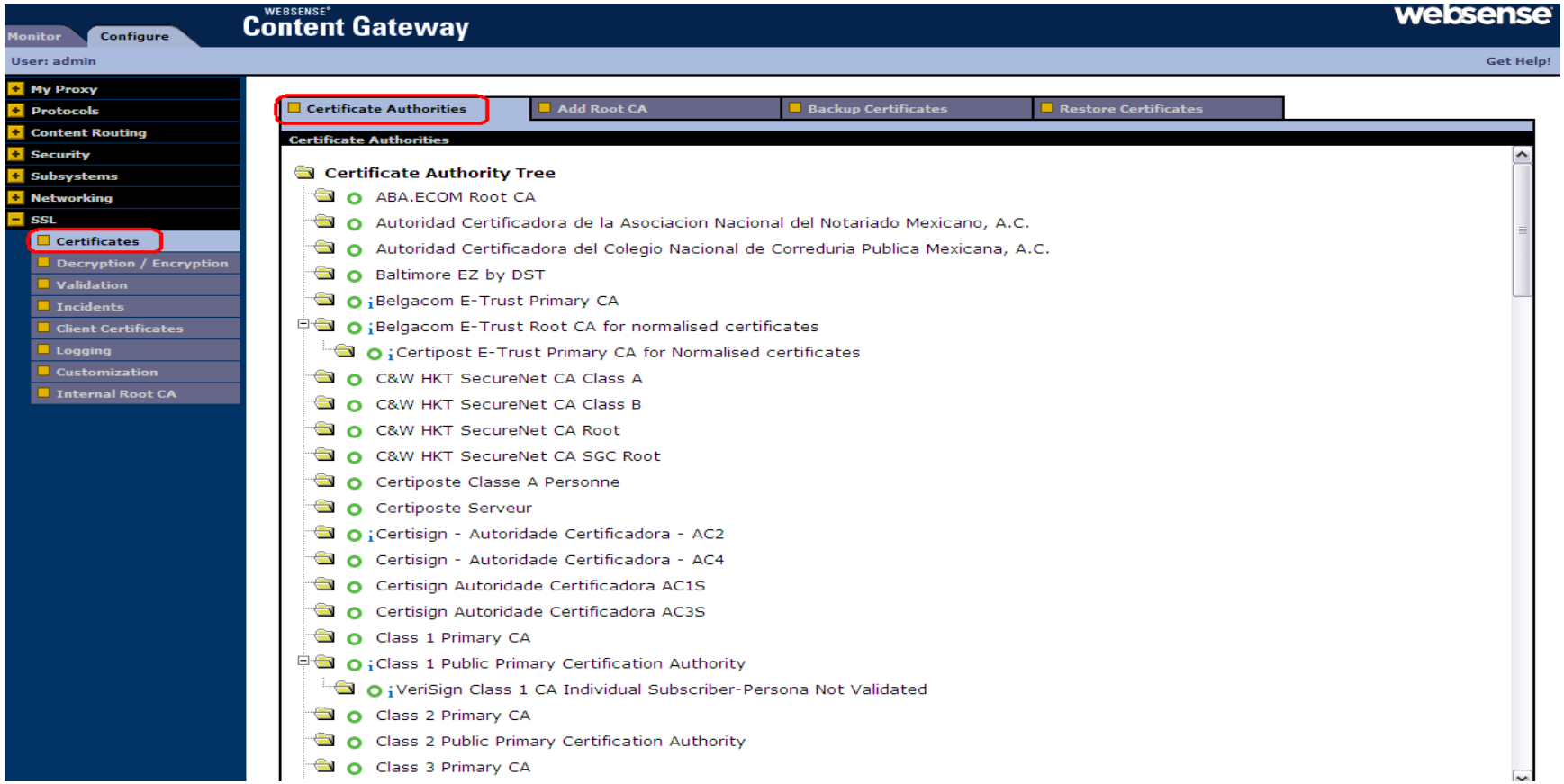
Certificate Management

Certificate Authority Tree

- SCIP comes installed with the same list of CAs as the standard web browser installation.
- Other CAs are automatically added when sites signed by them are visited.
- Sites can also be added manually.
- Users can delete, allow, and block individual CAs and Sub-CAs.

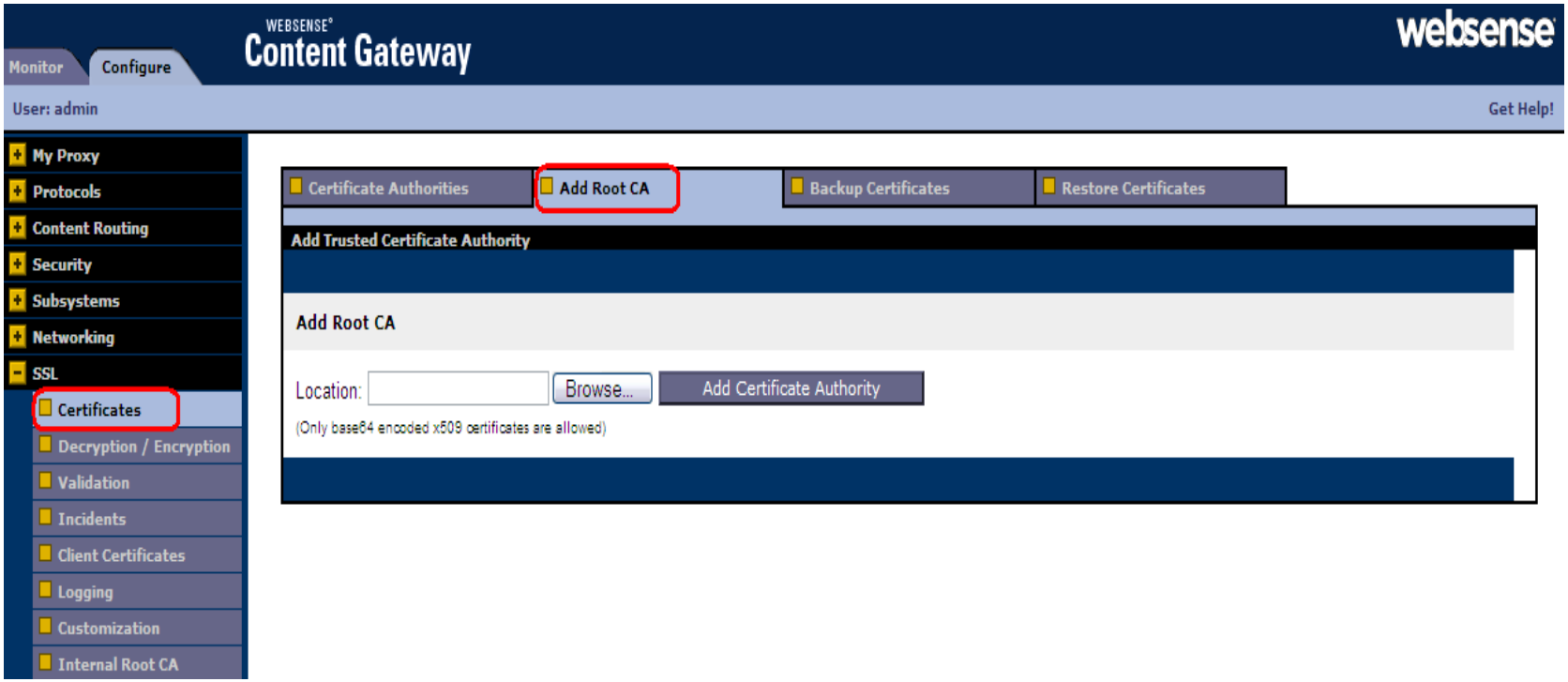
Certificate Authority Tree

- Used to manage all known root CAs, trusted CAs are listed
- New CAs are added automatically with denied state
- Selecting and clicking on the certificate allows changing the state



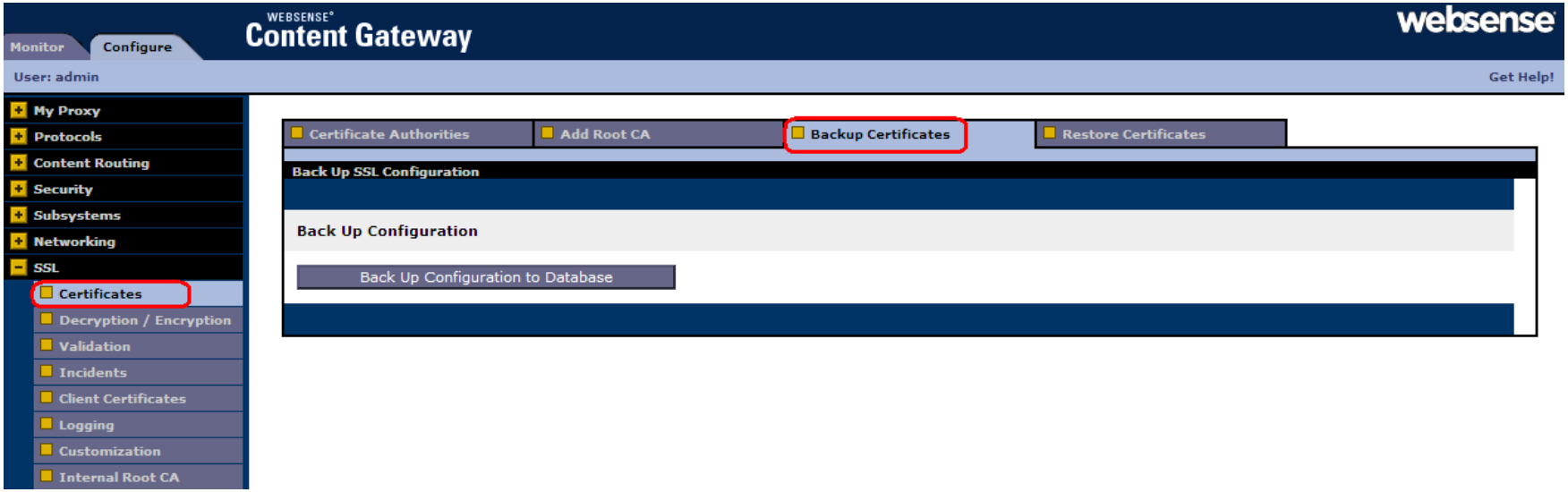
Add Root CA

- The certificate has to be in x509 Format and Base64 encoded.



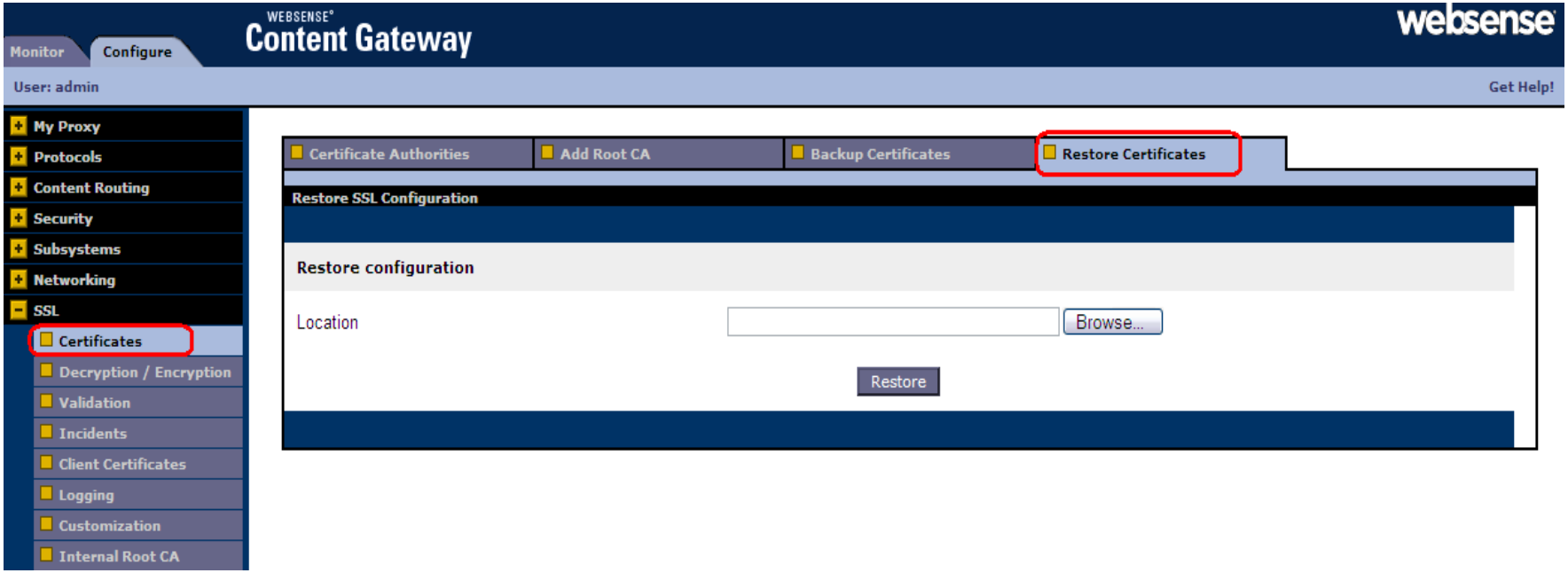
Backup Certificate

- The database can be saved(*.sdb format) to be used to restore the certificates in the future if needed.
- Click on Get copy of Database and save at the desired location.
- Use Restore Certificates Menu to restore the database



Restore Certificates

- Here you can restore the certificates backed up earlier.
- Browse and point to the location where database is saved and click Restore.

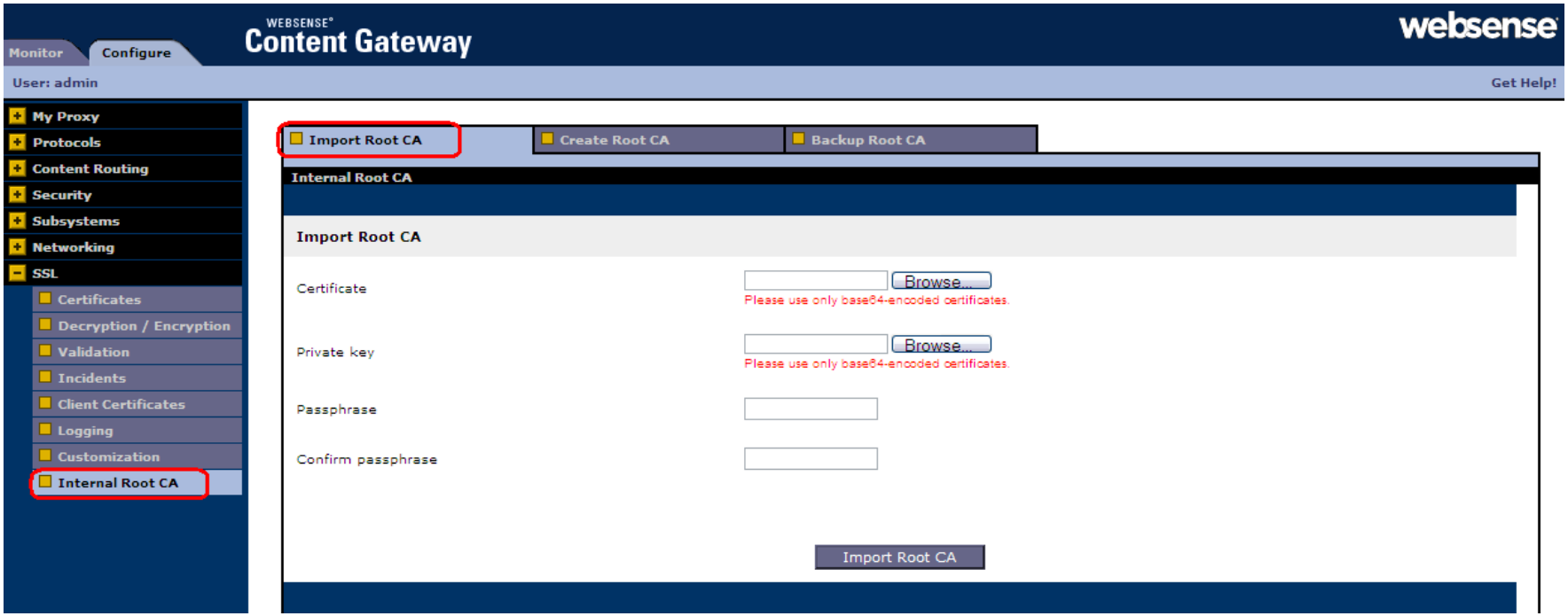


Internal Root CA

- This is the Certificate used by the WCG in response to client HTTPS requests.
- Deployment Options
- Import
  - Import a certificate already purchased from a CA.
  - Advantage of already being in all browsers.
  - The certificate and the private key has to be in x509 Format and Base64 encoded.
- Create
  - Create a new Internal root CA.
  - Will need to be deployed to all browsers (GPO)

Import Internal Root CA

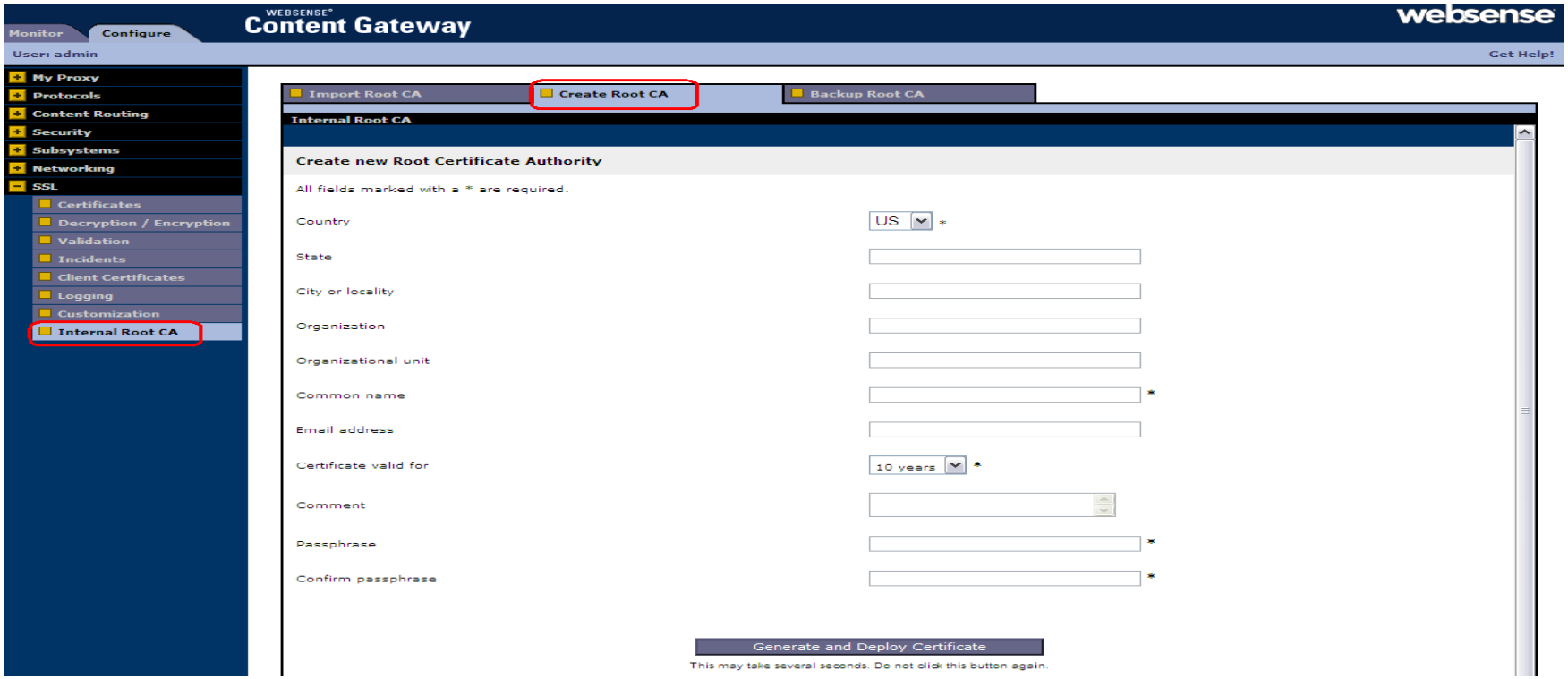
- If you want to use a different Root CA you can do this here.
- The certificate and the private key has to be in x509 Format and Base64 encoded.



Note: Restart of the WCG required.

Create Internal Root CA

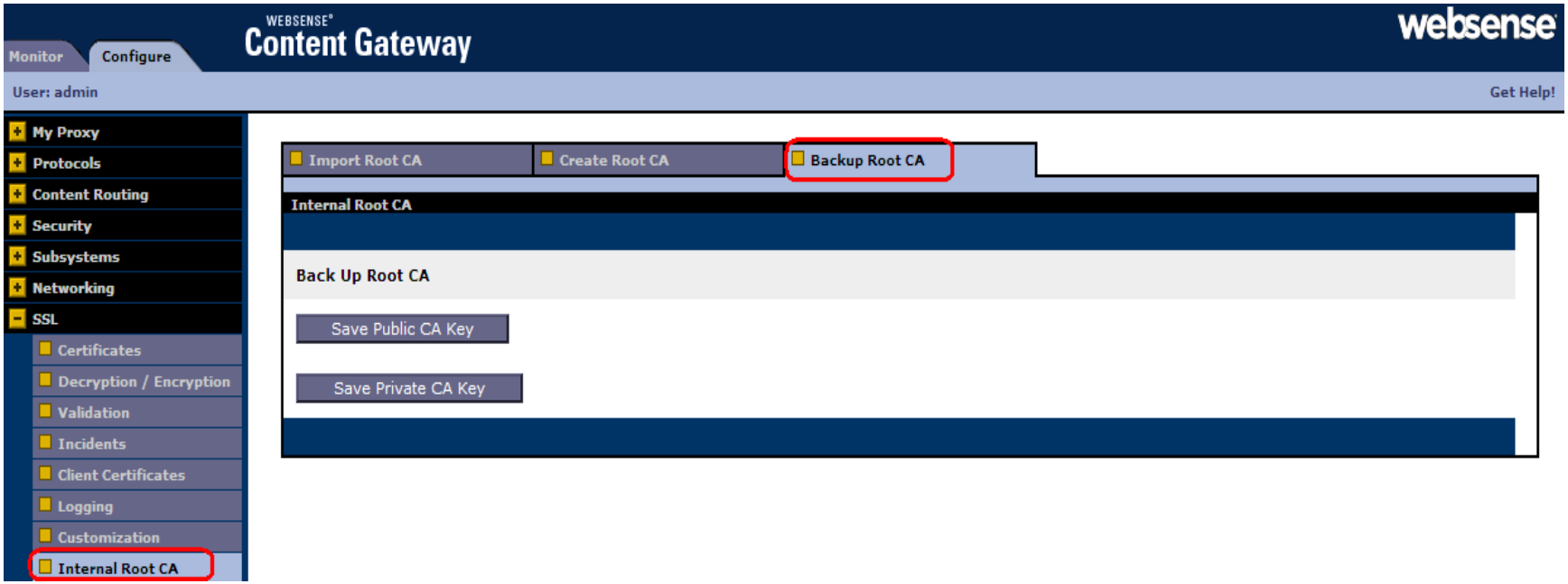
- Create internal Root CA.
- Creating a new Internal Root CA will invalidate any previously deployed Root CA.



Note: Restart of the WCG required.

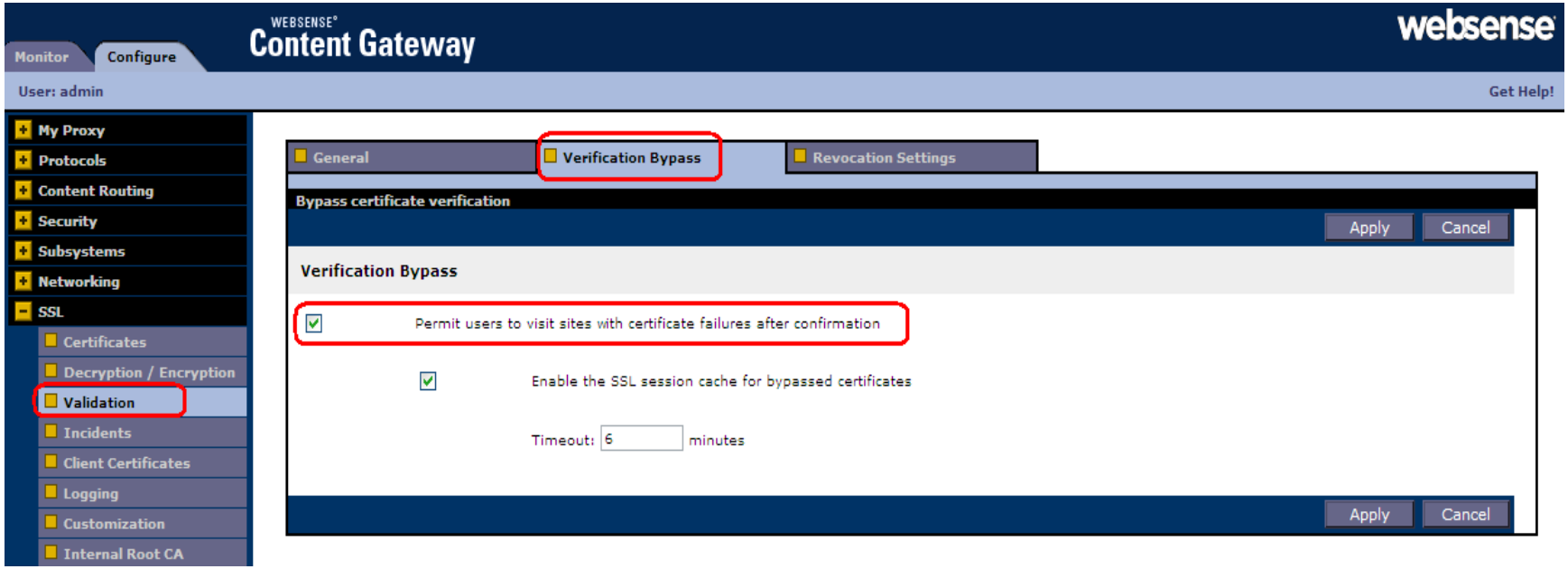
Backup Internal Root CA

- Once deployed, changing the root CA will cause HTTPS connection failures.
- Backup Internal Root CA for Failure recovery and Clustering support.



Verification Bypass

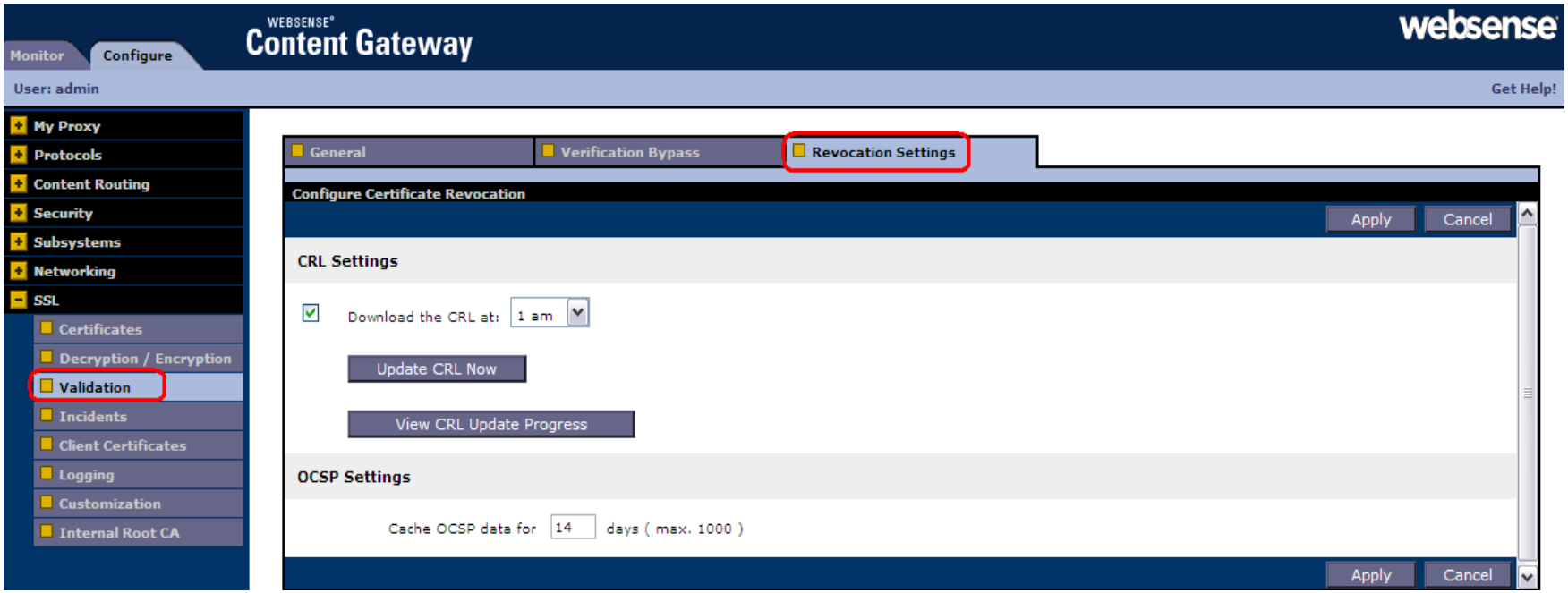
- Configure > SSL > Validation > Verification Bypass
  - Enables users to visit a site even if the certificate is invalid.
- Enable the SSL session cache for bypassed certificates
  - Store information about bypassed certificates in cache and reuse the connections.



SSL-Certificate Verify failed

Revocation Settings

- Configure > SSL > Validation > Revocation Settings
  - Configure how SSL Manager keeps revocation information current. By default, SSL Manager downloads CRLs on a daily basis.

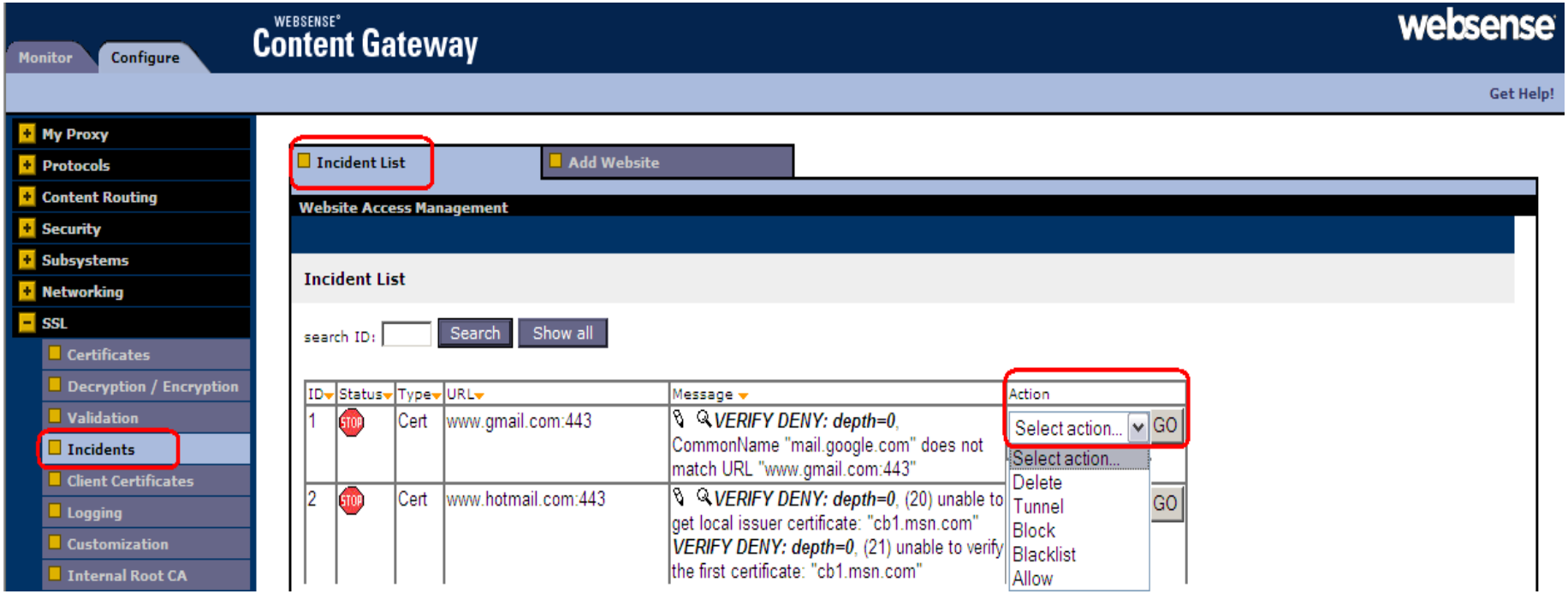


Certificate Revocation

- Reasons why certificate could become untrustworthy prior to expiration:
  - Compromised or suspected compromise of the certificate subject's private key.
  - Discovery that a certificate was obtained fraudulently.
  - Change in the status of the certificate subject as a trusted entity.

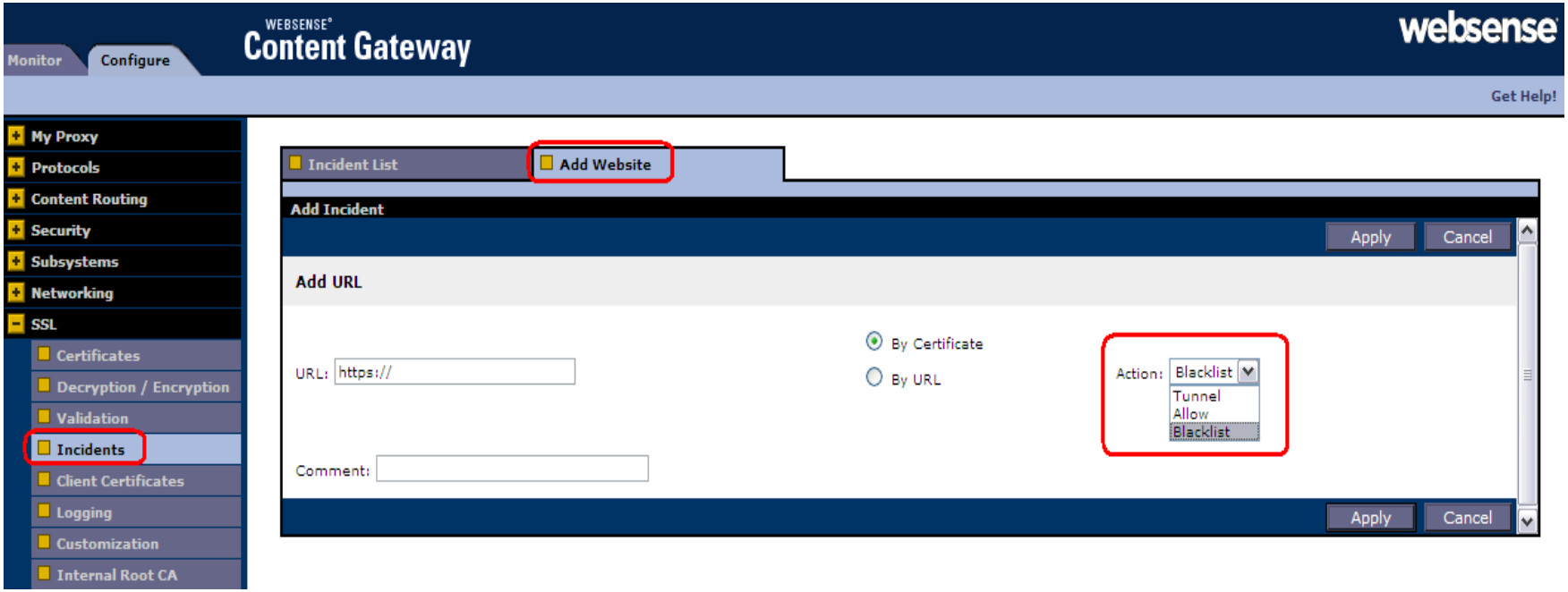
SSL Incident Management

- Configure > SSL > Incidents > Incident List
  - Sort by any field or search for an incident ID



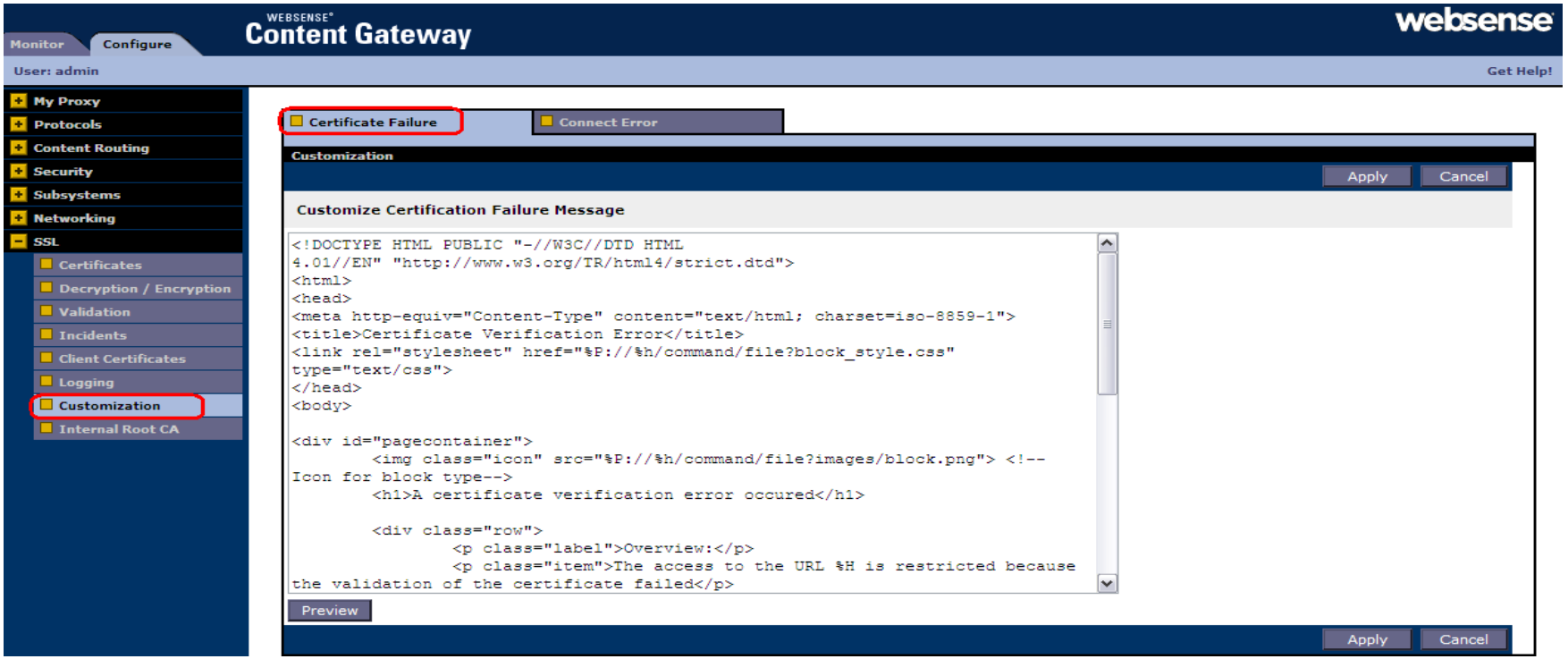
SSL Incident Management

- You can add incidents manually and configure the Action you want the SSL Manager to perform



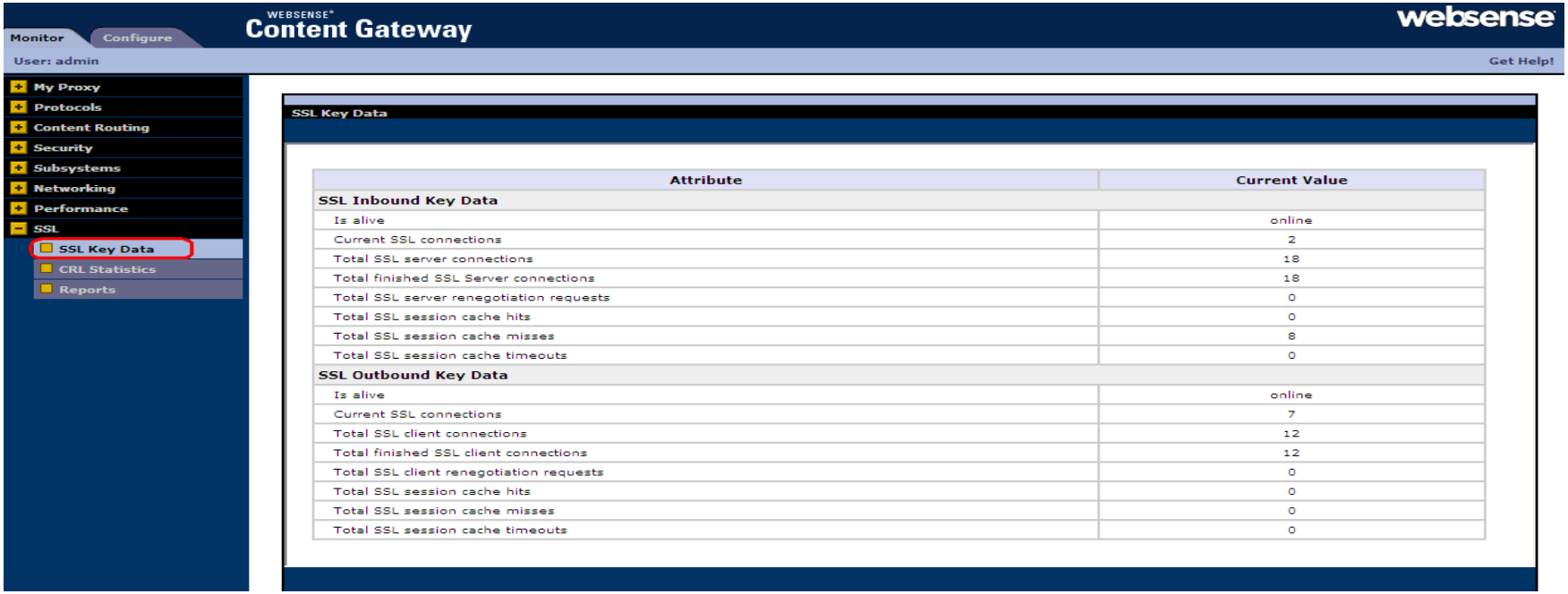
Customization

- Configure > SSL > Customization > Certificate Failure
- You can customize the message users receive when:
  - They are trying to connect to a site that has an invalid certificate.
  - There is a connection failure.



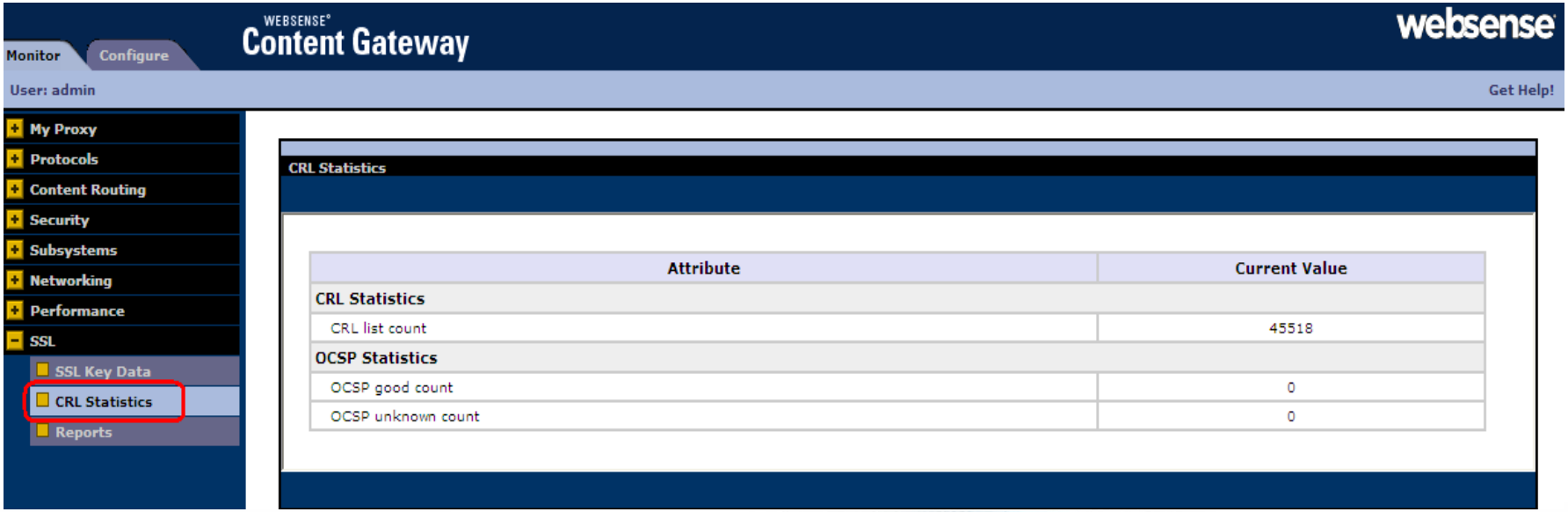
SSL Key Data

- Monitor > SSL > SSL Key Data
  - Provides information about the status of the SSL connection. and activity
  - Between the client and SSL Manager and SSL Manager and the destination server.



Certificate Revocation List

- CRL is the Certificate Revocation List
  - Provides statistics on certificate status
    - CRL - generally downloaded nightly
    - OCSP – Online Certificate Status Protocol
      - Checks certificate status online. Returns Current, Expired or Unknown



Summary

- SSL Overview
  - Digital certificates, Public/Private keys, CA's
- HTTPS Module Overview
  - SCIP, Proxy, Certificate Validation
- HTTPS Configuration
  - Enable HTTPS, Certificate Validation
- SSL Bypass
  - Incident management, manual
- Certificate Management
  - Create, Import, Backup Certs. and Internal Root CA

Support Online Resources

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

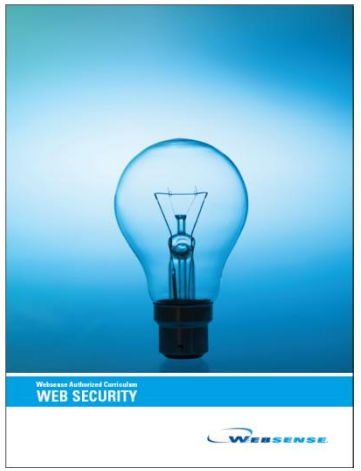
- Create and manage support service requests using our online portal.

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:
  http://www.websense.com/findaclass
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:
  readiness@websense.com

WEBSENSE® Authorized Training Partner

WEBSENSE® Certified Instructor



Webinar Announcement

websense
ESSENTIAL INFORMATION PROTECTION™

Upcoming Webinar

Title: **Troubleshooting, Logging and Reporting Issues for Websense Web Filter 7.x**

Date: **March 10, 2010**

Time: **8:00 AM PST**

How to register:

http://www.websense.com/content/SupportWebinars.aspx

Questions?

websense®
ESSENTIAL INFORMATION PROTECTION™