



A Websense White Paper

Compliance and Data Loss Prevention in Today's Regulatory Environments:

## The Value of Websense Email Security

### The Compliance Challenge

Over the last few years, governments around the world have taken an increasingly detailed interest in how organizations manage personal data. This has led to a rash of legislation, much of which requires corporations to take specific action to protect personal, identifiable information. Although each country's laws differ in specifics, compliance in each case often forces companies to address the protection of personal, identifiable information within the inward- and outward-bound communication channels. The extent of the challenge and the potential penalties of failure—fines, loss of business, reputation damage, and lawsuits—make compliance with these laws a critical item for the corporate governance agenda. Added to the already pressing need for acceptable use policy enforcement and protection of confidential information, regulatory compliance requirements are making the need for corporate governance immediate. Examples of mandatory regulations include:

- The Health Insurance and Portability Act (HIPAA) of 1997 requires that U.S. healthcare companies ('covered entities') implement 'hardware, software, and/or procedural mechanisms that record and examine activity...and that contain or use electronic protected health information' (164.312.b). This means that there must be appropriate controls and safeguards in place to protect any information that can be used to identify an individual and that relates to physical or mental health conditions, healthcare, or payment for healthcare. This information is known as Protected Health Information (PHI). For more information about technology's role in the protection of PHI, see the Websense® paper: Protecting Medical Privacy In a Digital Age: Beyond Policies and Procedures, A Critical Role for Technology: ([http://www.surfcontrol.com/uploaded\\_files/general/white\\_papers/HIPAA\\_Whitepaper.pdf](http://www.surfcontrol.com/uploaded_files/general/white_papers/HIPAA_Whitepaper.pdf))
- The Gramm-Leach-Bliley Act (GLBA) of 1999 protects consumers' financial information in the United States by requiring the implementation of processes to secure and protect personal consumer financial data from unauthorized access or use.
- The Sarbanes-Oxley Act (SOX) of 2002 requires that U.S. companies institute disclosure controls and procedures to ensure that the information they disclose in reports is accurately recorded, summarized, processed and reported within specified time periods. These controls and procedures are meant to provide reasonable assurance that the company's assets are safeguarded against unauthorized or improper use, and that its transactions are correctly recorded and reported.
- The Email Protective Marking Standard of the Australian Government requires that a protective marking be used to convey the security classification of information in an email message header, as defined within the Australian Government's Protective Security Manual(PSM).
- The United Kingdom's Data Protection Act of 1998 requires that appropriate security measures are in place to safeguard against unauthorized or unlawful access to or disclosure of personal data.

Corporations are expected to understand the rules and achieve compliance. Consequences of non-compliance include criminal and civil penalties, with more expensive fines for wrongful disclosure of confidential information where no compliance effort has been made. In addition to fines and/or imprisonment, there is also the potential for lawsuits and for harm to an organization's reputation. In fact, years of trust and goodwill can turn into mistrust and even hostility from the people who depend on the business they deal with to keep their confidential information private.

Corporations are increasingly expected to take greater responsibility for what their users do on the Internet. Acceptable use policies and protection of confidential information must already be addressed as part of the corporate governance compliance plan. Inappropriate use of corporate email or dissemination of intellectual property can result in consequences such as lawsuits, fines, loss of corporate reputation and goodwill.

Any comprehensive corporate governance plan must include a technology infrastructure that supports processes to ensure enforcement of corporate policies. The fact that email is the primary means of communication within companies, and between employees and the outside world, makes it the primary source of liability risk. Outgoing message security is a critical concern because unlike telephone or in-person discussions, email lives on over time and often contains valuable company or personal content. If your goal is sustainable compliance, Websense Email Security is an essential tool for successful management of corporate email. This document outlines the critical role that Websense Email Security plays in the enforcement of corporate policies regarding outbound email.

For the purposes of this guide, Websense Email Security for SMTP is abbreviated to "Websense Email Security." Throughout this document, Websense recommendations are noted in bold type.

## EMAIL POLICY IMPLEMENTATION

Email is the primary method of communication between organizations and individuals. Email regulatory compliance therefore depends on differentiating between legitimate and illegitimate email communications and taking action to restrict any illegitimate emails. Of course, for most organizations, their volume of email communication is so huge that it would be impractical to even try to manually review individual emails for compliance. The only effective method for dealing with the issue is to use email filtering solutions that are trained to differentiate between legitimate and illegitimate email communications. Controlling access therefore requires:

- A corporate email compliance policy. The significance and importance of this policy is such that it should form a significant part of the organization's corporate governance plan.
- A technical policy enforcement mechanism such as Websense Email Security, which comes with configurable rules and dictionaries.
- Encryption capabilities to help ensure data privacy such as the security and authentication offered by transport layer security (TLS) in Websense Email Security.

As part of your email policy development and implementation, you will need to identify documents that usually contain information that must be protected. Confidential documents can contain different types of protected data such as:

- Protected health information
- Personal financial information
- Corporate financial information
- Corporate confidential business or technical information

## TYPES OF CONFIDENTIAL INFORMATION

Legislators have been particularly concerned about protecting personal health and financial information, while simultaneously wanting to ensure that consumers are able to move between different financial and health care providers, and for their personal information to move with them. The conflict between these two concepts—restricted access to personal information and portability of personal information—make it virtually impossible for any organization to meet the regulatory requirements without deploying a technical solution.

## Personal Health Information

Electronic personal health information (PHI)—as defined in HIPAA Final Rule Part II, 45 CFR 164.501—includes individually identifiable information that relates to a person’s health, mental or physical health treatment, or payment for healthcare services. Examples of PHI include any combination of personal identifiers (such as patient name, account number or other identifying information) and healthcare treatment information such as an ICD-9 diagnosis code, an AMA treatment code, or the names of diseases or other health conditions.

## Personal Financial Information

Personally identifiable financial information—as defined in the GLBA Privacy Final Rule (n) 2—is either a combination of a personal identifier (name, account number, etc.), with financial information relating to that individual (such as stock prices, investment options or borrowing arrangements), or credit card information.

## Corporate Financial Information

Corporate financial data may include permissible, but prematurely released information, such as earnings statements, acquisition details, and quarterly statements.

## Corporate Intellectual Property

Email that contains information about corporate intellectual property that may not be ready for public release might include terms and phrases such as “design patent,” “trademark,” or “invention.”

Websense Email Security includes extensive and thorough dictionaries that are based on these types of identifiers. Depending on the legislation with which you would like to be compliant, you can enable the associated default compliance rules.

## HOW WEBSENSE EMAIL SECURITY CAN HELP

Websense Email Security provides out-of-the-box compliance rules to help prevent data leakage in email and help ensure regulatory compliance, as well as many options for handling outbound messages. This document offers a variety of recommendations about how to configure Websense Email Security to protect confidential information. You are encouraged to choose the recommendations to best enforce your company’s email policies. For example, the versatility of Websense Email Security allows you to block outbound messages containing confidential information. You can allow only encrypted messages to be sent to trusted partners. You can also add a banner containing a unique expression to each message, notification via email about policy violations, and so on. Protecting confidential information in outbound email requires:

1. Monitoring of outbound email and detecting any message that contains sensitive information.
2. Taking action on each message based on Websense Email Security rules.
3. Reporting and analysis of email policy enforcement.

## CONTENT FILTERING: RULES AND DICTIONARIES

Websense recommends that you enable the default compliance rules and customize the related dictionaries to achieve maximum effectiveness for your unique organization.

### Dictionaries

Websense Email Security comes with a variety of pre-configured dictionaries, including specially designed compliance dictionaries. The flexibility and versatility of the dictionaries enable you to specify exact matches, and use wildcard characters.

You can also create custom dictionaries. Twenty different user-defined dictionaries can be customized to protect confidential information, and with thirteen dictionary language packs covering seventeen different risk categories, Websense Email Security makes content filtering easy.

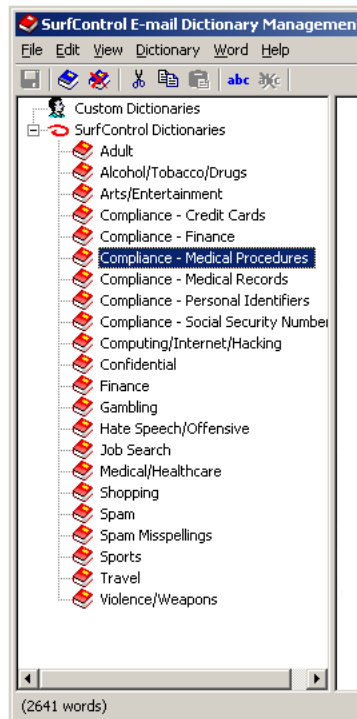
## Compliance Dictionaries

Websense Email Security can help your company comply with both HIPAA and GLBA because it can recognize personally identifiable information with its four specially designed compliance dictionaries:

- Personal identifiers
- Medical procedures
- Finance
- Credit cards

You can also use the Personal Identifiers dictionary and the Credit Cards dictionary to help comply with Canada's PIPEDA or the U.K.'s Data Protection Act. These dictionaries work together, or in isolation as required, to help protect your data and stay in compliance with these regulations. To access the Compliance dictionaries, click the Dictionary Management tab. The full list of dictionaries is shown in Figure 1.

Figure 1.



If there is an audit, the fact that you are using the compliance dictionaries in Websense Email Security can serve as evidence of your compliance efforts. Specifically, the product's dictionaries and rules assist you in providing the compliance necessary to protect your employees, your information and your business.

Websense recommends that you enable the default compliance rules. This will enhance the compliance dictionaries by adding unique industry- and organization-specific words and phrases that your risk assessment indicates should also be monitored within the context of your focused compliance efforts.

## Ensuring Medical and Healthcare Privacy

The HIPAA Privacy Rules define Protected Healthcare Information (PHI) as information that relates to an identifiable individual's health (diagnoses, diagnosis codes, etc.), healthcare (treatment plans, prognosis, etc.), or healthcare payment information. If in violation of the privacy rule, email will contain two types of confidential information that can be detected by Websense Email Security:

- Information that identifies a specific person such as a name, address, or driver’s license number. These entries are found in the personal identifiers dictionary
- Health, healthcare, or healthcare payment information such as diagnoses, treatment, or account numbers that are related to a particular person.

These terms are located in the medical procedures dictionary. The HIPAA and Personal Identifiers dictionaries in Websense Email Security are combined to help achieve compliance. Email messages that contain terms from only one of the dictionaries (personal identifiers or medical procedures) pass through the email filter because they do not violate the HIPAA Privacy Rule. Email messages that contain terms from both dictionaries are automatically isolated. The HIPAA Isolation Rule is therefore configured as medical procedure + personal identifier = isolate.

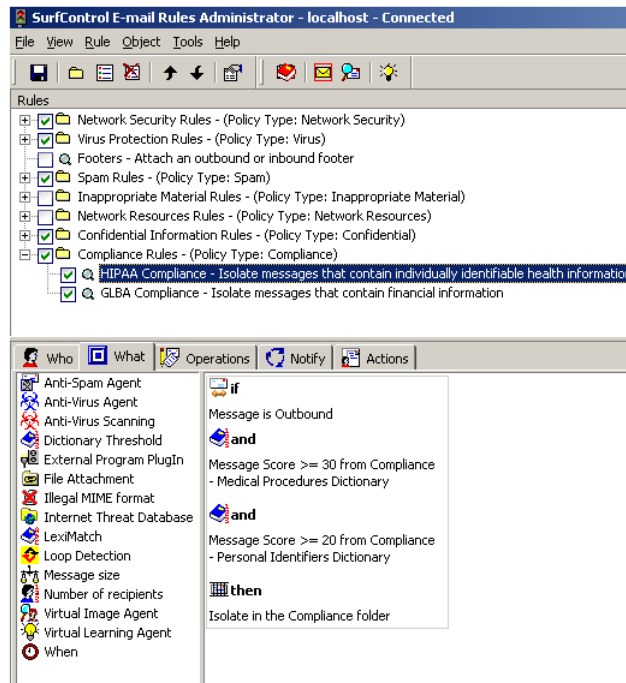
To help enforce GLBA compliance, the Finance and Credit Card dictionaries are used in conjunction with the Personal Identifiers dictionary in the Websense Email Security GLBA compliance rule. GLBA defines confidential data as any data that contains both a personal identifier and a financial term OR a credit card number.

### Compliance Rules

As you can see, Websense Email Security offers two different pre-configured compliance rules: one for HIPAA compliance and the other for GLBA compliance. The HIPAA rule helps comply with healthcare regulations in the U.S. and the GLBA rule helps comply with financial regulations in the U.S., Canada, and the U.K. Figure 1 shows the HIPAA compliance rule default configuration.

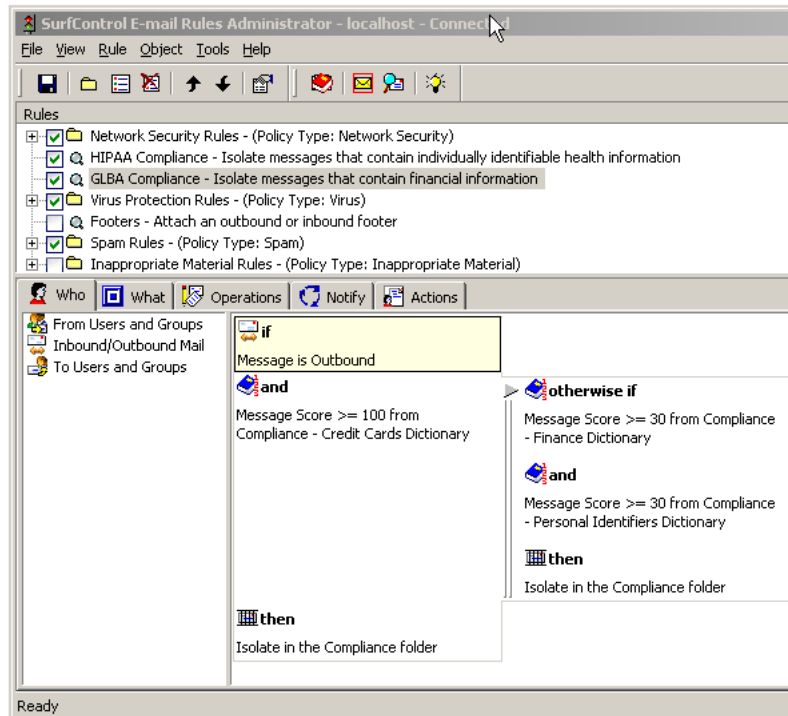
The basic HIPAA rule logic is that if a personal identifier and a HIPAA term are found together in the same email, then that email should be isolated. This rule helps ensure that private patient, healthcare, dental, or medical procedure information will not leave your network, and will be quarantined for further review. You can edit the action Websense Email Security takes on the message through the Actions and Operations tabs in the Rules Administrator. See Figure 2 for the default HIPAA rule set.

Figure 2.



The basic GLBA rule logic is if a personal identifier and a GLBA term are found together, OR if the email contains a credit card number, then isolate the email message. This rule helps ensure that private financial information will not leave your network, and will be quarantined for further review. You can edit the action Websense Email Security takes on the message using the Actions and Operations tabs in the Rules Administrator. See Figure 3 for the default GLBA rule set.

**Figure 3.**



## RULE PLACEMENT

When Websense Email Security processes an email, it checks the message against each of the rules in order, starting at the top of the screen until the email reaches a terminating action (Allow, Delay, Discard or Isolate). When it reaches a terminating action, the message is not checked against subsequent rules.

Rule placement therefore affects which email triggers a given rule, and which emails are allowed to reach their destination. **Websense recommends that you place the Compliance rule after the Spam rules and before the Inappropriate Material rules.** Also, if your compliance policy allows only specified employees to send email containing certain confidential information, place this rule in the Rules list before the other compliance rules that apply to everyone at the company.

## OTHER WAYS TO USE EMAIL FILTER FOR COMPLIANCE

### Compliance Templates

**To optimize your catch-rate of confidential documents being sent via email, Websense recommends that you create standard document templates.** Document templates not only allow you to standardize the presentation of information, but also serve as a very effective weapon in the compliance war. Templates can compartmentalize personal data into fields that can be easily detected by Websense Email Security. In the

event of an audit, the use of compliance document templates will serve as further evidence of your efforts to meet compliance regulations. To create compliance document templates:

1. Identify the forms and documents commonly used in your organization that contain confidential information.
2. Create a template for each type of document, creating a named field for each piece of confidential information. For example, you could name the field containing the earnings per share figure, "Earnings Per Share."
3. Create or edit an existing dictionary and add the field names you want to filter, assigning each a value of 100.
4. Create a Websense Email Security rule that looks for the field name in email messages and attached documents.

You might also code your templates in the following ways:

- Add a header that includes a unique identifier in white text to each template. For example, "XH2973."
- Create or edit an existing dictionary and add the unique identifier, assigning it a value of 100.
- Create a rule that looks for the unique identifier in email messages and attachments. Although the identifier will not be visible to readers, any email containing the identifier will trigger the rule.

### Seeding Customer Lists

In cases where lists of customer names are being sent in email, you may want to add one or more names that are not real customer names. You can then configure a Websense Email Security rule to look for these particular names in messages and isolate these messages if they are not sent to a specified recipient. See the "Sending to Specified Recipients" section below for more information.

Using the Rules Administrator's easy drag-and-drop interface, you can easily create filtering rules that specify the way email is checked and processed. You can even enable decompression of encrypted and password-protected files with the Rules Administrator's Password Protected Archives feature. Websense recommends that you use your corporate policies as a reference when you configure rules in order to provide comprehensive content filtering. Websense also recommends that you use the Rules Administrator to backup your Rules set whenever you make a change to one or more rules.

### Using PEM for Outbound Compliance Verification

You can use Personal Email Manager (PEM) as a screening for outbound compliance-related messages. By configuring PEM to notify the sender (or the sender's manager) if a compliance rule is triggered, you are establishing effective checks and balances within your email infrastructure that helps ensure sensitive data is handled appropriately.

### Entering Personal Information

Companies ("covered entities") with a limited amount of personal health information (PHI) or customer-limited financial information may choose to manually enter it into a custom or existing dictionary. An example of this would be a long-term care facility with a limited number of patients. In this case, actual patient names, social security numbers, or account numbers can be entered into a dictionary and used with a rule to block all email containing that information. **Websense recommends that this method be used where possible because it is the most reliable method of protecting email containing very specific data such as patient names, which cannot otherwise be blocked using a rule set.**

## Outbound Email Disclaimer

The Footer rule in Websense Email Security is another very effective tool you can use as evidence of your compliance effort and to help reduce liability. **Websense recommends that you configure the Footer rule to append a standard disclaimer to all outbound confidential email.** The footer rule's default message is shown below and can be customized:

"This email and any files transmitted with it may be confidential and are intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the originator of the message."

## Specifying Recipients

Specifying recipients allows you to block and isolate any confidential email that is not sent to an approved user, group, or domain. Websense recommends that you specify recipient domains when sending confidential email to business partners such as insurance companies, accounting firms, or healthcare providers.

## Specifying Delivery Time Frame

The end of quarter or fiscal year is a "quiet period" for many companies when certain corporate information shared with the public can subject the company to fines and penalties. Prior to the beginning of the quiet period, Websense Email Security can be configured to isolate any email that may violate corporate confidential information policies. Once a cut-off date is established, you can create a rule that checks all outbound email that arrives during a specified date and time period for terms or phrases from the Confidential dictionary. If the message meets the dictionary threshold, the message is isolated in the Confidential folder.

## The Virtual Learning Agent

The Virtual Learning Agent (VLA) is a powerful tool that you can train to recognize the kind of content you want to detect and block such as confidential documents. Using documents that contain the content you want to detect (the category) and documents that do not contain this type of content (the counter category), you can train the VLA object before using it in rules. The VLA workflow consists of:

- Adding a category name and description
- Adding documents to the category
- Adding documents to the counter category
- Training the VLA
- Testing the VLA using additional documents

Websense Email Security has a built-in VLA tutorial and a set of examples to familiarize you with using the VLA object in rules. See the Websense Email Security Administrator's Guide for more information on training the VLA.

## Smart Host Routing

Depending on how your network is configured for compliance and security, you may already have certain compliance-related servers in place. For example, if your security policy mandates desktop-to-desktop encryption, you may use an encryption server. Your network may also include an archiving server, which provides email storage and retrieval.

If you are using a third-party encryption or archiving server, Websense Email Security easily integrates into your existing routing scheme. Websense Email Security can instantly forward email (or copies of email) to your encryption or archiving server once you configure the Smart Host Routing object within your Websense Email Security rule set. Not only does this object allow you to route email between your Websense Email Security server and other compliance servers, but you can specify the routing to occur based on email content, sender, recipient, domain, etc.

For details on how to configure Smart Host Routing, refer to Knowledge Base article 1690, which specifies both how to set up the Smart Host route and how to add that route into a rule.

## Encryption

Some privacy regulations (such as HIPAA) specify that confidential data must be transmitted in a secure or encrypted format. Since basic SMTP does not include encryption or authentication, Websense Email Security supports Transport Layer Security (TLS) and secure SMTP (SMTPS).

## TLS

TLS enables encryption along SMTP connections, and helps ensure that no third party can eavesdrop or tamper with any message. TLS allows the sending and receiving servers to authenticate each other using digital certificates and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. If you are using a POP or IMAP email client that supports TLS (all modern ones do), all mail sent from your client to the mail server will be encrypted. **Websense recommends activating TLS encryption for all confidential email sent to business partners.**

## SMTPS

Secure SMTP (SMTPS) is another feature that's available in Websense Email Security. SMTPS is similar to TLS but uses Secure Socket Layer (SSL) version 3.0 for all communications and encrypts the entire session using a different default port (465). It also requires a digital certificate.

## Digital Certificates

To activate a digital certificate, you can install an existing certificate, create a self-signed certificate, generate a Certificate Signing Request (CSR), or process and install a signed certificate. All certificates reside in the Windows Certificate Store (.keystore) file. See Knowledge Base article 1804 for more information on obtaining digital certificates. Since some companies have a policy of only sending to business partners who have an independently supplied (CA) certificate, Websense recommends that you agree on the type of certificate required by your partners prior to using a self-signed certificate.

## Archiving

Certain compliance regulations require that communication records be retained for a specified amount of time. If your organization uses an archiving server, Websense Email Security integrates with it using Smart Host Routing. Using the Smart Host Routing Redirect function, copies of email that meet your archiving criteria can be sent to the archiving server while the original email is processed normally.

## Notification

There are various email notification options available in Websense Email Security that can be customized. Notification email enables corporate management, individual employees, and/or human resources to be informed about policy violations as needed. Using notification email, you can notify employees when they violate policy, and management or human resources can track policy violations to identify repeat offenders and take appropriate action.

## Monitoring and Detection

Effective enforcement of corporate compliance policy is dependent upon accurate detection of confidentiality violations within outbound email. You can track the progress of emails through Websense Email Security using the Monitor. In addition to server and queue statistics, the Monitor shows the status of the Receive, Send and Rules services. The Monitor's Message Administrator feature enables you to view and manage your queues.

## Auditing and Reporting

Accurate and relevant reports provide essential overviews of email messaging security at your company, and are required in case of compliance audits. Websense Report Central offers real-time auditing and provides a comprehensive view of your company's compliance enforcement. Report Central offers both standard reports and the ability to create custom reports that offer an in-depth view of how email is

being used at your company. You can even delete reports to maximize your archiving space. Websense recommends that auditing reports be scheduled to run at regular intervals, automatically delivered to specified mailboxes, and archived using the Archive Reports option in Report Central.

## Rules Reports

The Rules Reports show you which rules are being broken, by whom, and how often. To track incidents where Websense Email Security compliance rules are being triggered, run reports on the internal users who are triggering these rules.

You can also create custom reports using criteria that you specify. These reports can subsequently be generated many times without having to re-enter the criteria. By selecting the Report Criteria tab in Report Central, you can specify what users, groups, sites, categories, or protocols to include (or exclude) in a report. When you run a search for these criteria, and you can limit the number of results by entering a number in the Retrieve N criteria, where  $N < 2000$  field.

Additionally, you can use a third-party reporting tool such as Crystal Reports to create reports from the Websense Email Security STEMlog database.

## References

### **Protecting Medical Privacy in a Digital Age: Beyond Policies and Procedures, A Critical Role for Technology**

[http://www.surfcontrol.com/uploaded\\_files/general/white\\_papers/HIPAA\\_Whitepaper.pdf](http://www.surfcontrol.com/uploaded_files/general/white_papers/HIPAA_Whitepaper.pdf)

### **Achieving Compliance: Best Practices for Outward Bound Internet Content Protection**

<http://www.surfcontrol.com/go/WPcompliance>

### **Knowledge Base article 1690, Smart Hosting Routing Set Up Instructions**

<http://kb.surfcontrol.com/article.asp?article=1690&p=5>

### **Knowledge Base article #1804, About Digital Certificates**

<http://kb.surfcontrol.com/article.asp?article=1804&p=5>

### **Knowledge Base article #, Examples of How to Configure Websense Email Security for Compliance**

<http://kb.surfcontrol.com/article.asp?article=1807&p=5>