**Rapid Deployment Kit: Phase 4**

**Web DLP Configuration**

One of the key features of Websense Web Security Gateway Anywhere is that it includes Websense Data Security technologies to prevent data loss over the Web.

This means that you can protect whatever data you deem vital from leaving your organization by the Web—this includes HTTP, HTTPS, FTP, and FTP-over-HTTP. Depending on your needs, you can monitor or block the unwanted transmission of vital data, and you can send notifications and alerts when policy breaches occur.

In addition, you can create DLP policies that base rules on URL categories.

The following steps describe how to enable DLP over Web channels.

1. **Install Data Security Manager:**

Data Security software should be installed on its own Windows 2003 machine.

The machine where you install the software is called the *Data Security Management*

*Server*. This machine provides Web Security Gateway Anywhere’s core data loss

prevention technology, capturing fingerprints of your data, applying policies, and

storing incident forensics.

For instructions on installing Data Security software, refer to [*Installing the Software*](http://www.websense.com/content/support/library/shared/v75/wsga_getting_started/inst_sw_dss.aspx), on page 70 of the Web Security Gateway Anywhere Getting Started Guide. For instructions on installing Data Security on a VM, see [*Installing on a virtual machine*](http://www.websense.com/content/support/library/shared/v75/wsga_getting_started/vm_install.aspx), on page 72 of the WSGA Getting Started Guide.

1. **Install Linking Service**

Websense Linking Service makes it possible for Websense Data Security to access user information and URL categorization details from Websense Web Security.

When installing Linking Service separately, be sure that Filtering Service, User Service, and a transparent identification agent (DC Agent, Logon Agent, or RADIUS Agent) are already installed and running.

To install Linking Service, see [Installing hybrid and Web DLP components](http://www.websense.com/content/support/library/shared/v75/wsga_getting_started/hybrid_dlp_inst.aspx) (For Web DLP functionality, you do not need to install Directory Agent or Sync Service, just Linking Service).

1. **Register the proxy with the Data Security module**

To enable data loss prevention over Web channels, you must connect the Content Gateway module of your Web security solution to the Data Security Management Server. For steps to establish that connection, see [*Registering the proxy with the Data Security module*](http://www.websense.com/content/support/library/shared/v75/web_dlp/proxy_dss.aspx).

**Note**Data Security is not connected to your Content Gateway module until you log onto TRITON – Data Security and deploy the settings.

✓

1. **Link Data Security with Linking Service (WWS)**

To get the full benefit of Web DLP, you need to configure linking between the Web and data security modules.

See [*Configuring linking between Web and data Security*](http://www.websense.com/content/support/library/shared/v75/wsga_getting_started/link%20config.aspx), on page 93 of the Websense Web Security Gateway Anywhere Getting Started Guide.

1. **Integrate Active Directory (If not already configured)**

If your organization uses a supported directory service, you can configure Websense

Web Security Gateway Anywhere to:

* Apply policies to directory clients (users, groups, and domains [OUs])
* Include information about directory clients in reports
* Allow administrators to log on to the TRITON Unified Security Center using their

network accounts

To configure Websense software to communicate with your organization’s directory service, see [*Configuring directory service settings*](http://www.websense.com/content/support/library/shared/v75/wsga_getting_started/configure%20dir.aspx), on page 88 of the Websense Web Security Gateway Anywhere Getting Started Guide.

1. **Import Users/Group from the Directory Service**

If you have one or more user directory servers, such as Microsoft Active Directory or Lotus Domino, you should integrate your servers into Websense Data Security configuration. Once you have set up server details and imported users and groups using TRITON - Data Security, you can base your administrator login authentication on user directory credentials, resolve user details during analysis, and enhance the details displayed with the incident.

If you did not set up your user directory server settings as part of your initial Websense Data Security configuration, see [Configuring user directory server settings](http://www.websense.com/content/support/library/data/v753/install/userdir_settings.aspx), on page 146 of the Data Security Deployment and Installation Guide.

By default, Websense Data Security imports data from user directory servers daily at 3:00 am. To change the import time, see [Importing user data](http://www.websense.com/content/support/library/data/v753/install/import_userdata.aspx), on page 147 of the Data Security Installation and Deployment Guide.