# Getting Started with the Symantec™ Data Loss Prevention Cloud Detection Service for Web Security Service (WSS)

Version 15.x

Symantec™
A Division of Broadcom

# Getting Started with the Symantec Data Loss Prevention Cloud Detection Service for WSS

Documentation version: 15.7

## Legal Notice

Broadcom
1320 Ridder Park Drive
San Jose, California
95131

https://www.broadcom.com

# Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

## Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

## Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

# Contents

Chapter 1

# Introducing and deploying the Symantec Data Loss Prevention Cloud Detection Service for WSS

This chapter includes the following topics:

# About the Cloud Detection Service for Web Security Service (WSS)

The Symantec Data Loss Prevention Cloud Detection Service for Web Security Service (WSS) is a Symantec Data Loss Prevention detection service deployed in the cloud that enables you to monitor content and identify information policy violations in cloud applications. Use the Symantec Data Loss Prevention Cloud Detection Service for WSS to integrate Symantec Data Loss Prevention with the Symantec Web Security Service (WSS), to inspect outbound HTTP/S and FTP content passing through your WSS cloud proxy.

Policy violations identified through the Symantec Data Loss Prevention integration with Symantec WSS appear in **Network** incident reports in the Enforce Server administration console.

Symantec manages and maintains the Cloud Detection Service. Your organization manages the Enforce Server.

You must purchase Symantec WSS separately.

For information about using the Symantec Cloud Detection Service to integrate with Symantec CloudSOC or other cloud applications, see the *Getting Started with the Cloud Detection Service* guide at https://www.symantec.com/docs/DOC9414.

# About this guide and additional documentation

This guide details what you need to know to use the Symantec Data Loss Prevention Cloud Detection Service. It also includes information about integrating Symantec Data Loss Prevention with Symantec WSS.

You can find installation, initial setup, and administration details for all aspects of Symantec Data Loss Prevention in the following guides:

- *Symantec Data Loss Prevention Administration Guide* at https://www.symantec.com/docs/DOC9261
- *Symantec Data Loss Prevention System Requirements and Compatibility Guide* at https://www.symantec.com/docs/DOC10602.
- *Symantec Data Loss Prevention Installation Guide* at https://www.symantec.com/docs/DOC9257
- *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide* at https://www.symantec.com/docs/DOC9259
- *Symantec Data Loss Prevention Release Notes* at http://www.symantec.com/docs/DOC10600

This guide may be updated periodically. To ensure that you have the latest version see the Symantec Support Center article at www.symantec.com/docs/ DOC10659. You can subscribe to the article to receive notifications when a new version of the guide is available.

# Cloud Detection Service for WSS release notes

This section includes known issues for the Symantec Cloud Detection Service for WSS.

**Table 1-1** Known issues with the Cloud Detection Service for WSS

| Issue ID | Description | Workaround |
|---|---|---|
| 4169789 | Symantec Data Loss Prevention fails to redact or block Yahoo Mail where policies include the **Network Prevent: Remove HTTP/S Content** response action with the **Network Prevent: Block HTTP/S** response action as fallback. | None. |

# About the Cloud Management Portal

The Cloud Management Portal is where you configure and keep track of your Symantec Data Loss Prevention cloud services. After you order a Symantec Data Loss Prevention cloud service, you receive an email from Symantec order processing. This welcome email tells you how to log on to the Symantec Data Loss Prevention Cloud Services Cloud Management Portal (CMP). After you get your service started, you can then use this guide to connect your new cloud service to your existing Enforce Server, through the Enforce Server administration console.

After you provide information about your requested services and press **Configure** in the CMP, Symantec sends you an enrollment bundle, in the form of a zip file. You will receive this enrollment bundle by the end of the next business day. You can then save this bundle to your Enforce Server.

# About roles for implementing the Cloud Detection Service for Web Security Services (WSS)

Several people in your organization may need to coordinate activities during the implementation of the Symantec Data Loss Prevention Cloud Detection Service. Although you may have different labels for each of these roles, or responsibilities may overlap, you should understand the different roles and associated activities for any individuals participating in the implementation process.

**Table 1-2** Implementing the Cloud Detection Service for WSS: roles and responsibilities

| Role | Typical responsibilities |
|---|---|
| Symantec WSS Administrator | May be a user of the Cloud Management Portal.<br>Configures the Symantec WSS solution.<br>The Symantec WSS administrator is usually part of a large administration team, and in charge of all WSS tasks. This administrator may or may not be the same as the DLP administrator. |
| DLP Administrator | May be a user of the Cloud Management Portal.<br>Installs licenses and registers the Cloud Detection Service for WSS in the Symantec Data Loss Prevention Enforce Server administration console. Configures system management and roles and configures detectors. May create policies, remediate incidents, monitor the user risk summary, and generate reports. |
| Network Administrator | Enables access from the Enforce Server to the Symantec Data Loss Prevention cloud service gateway. |

# Cloud Detection Service solution architecture and process flow

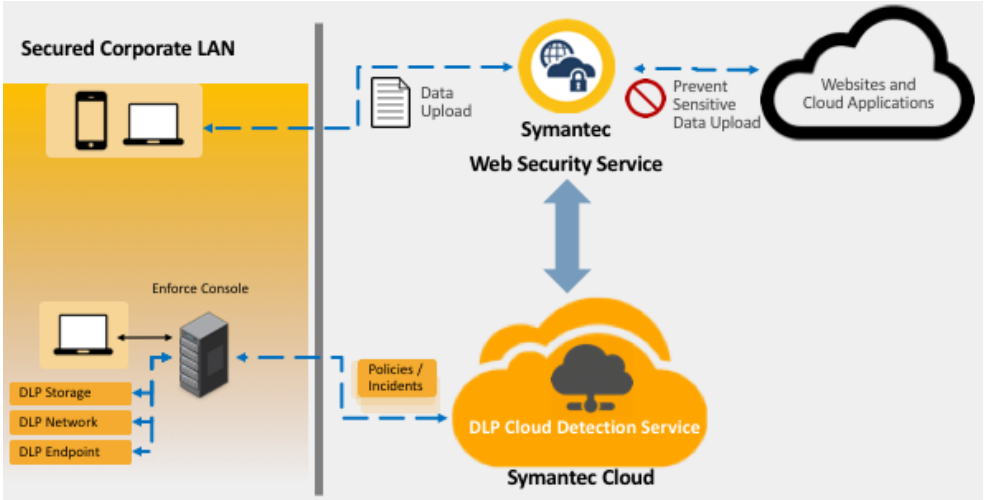
The Symantec Data Loss Prevention Cloud Detection Service solution consists of the following components:

- Symantec Data Loss Prevention 15.x on-premises Enforce Server and Oracle server.
- Hosted, Symantec-managed Cloud Detection Service for WSS that provides Symantec Data Loss Prevention capabilities.
- Symantec WSS cloud web proxy.

**Note:** Symantec WSS is purchased separately from the Cloud Detection Service for WSS and Symantec Data Loss Prevention.

Figure 1-1 shows the architecture of the Cloud Detection Service when it is integrated with WSS:

**Figure 1-1** Cloud Detection Service for WSS integration




# System and deployment requirements

The following items are necessary for deploying the Symantec Data Loss Prevention Cloud Detection Service for WSS:

- A completed provisioning form, returned to Symantec. Your sales representative provides you with the provisioning form when you place your order. It includes information about your organization and environment that Symantec requires to set up the Cloud Detection Service for WSS for you.
- A Symantec Data Loss Prevention Enforce Server and an Oracle database.
- An enrollment bundle for the Cloud Detection Service for WSS. Symantec sends your organization this enrollment bundle.
- An active Symantec WSS account. Your organization is responsible for purchasing, licensing, and maintaining Symantec WSS.

# Process for deploying the Cloud Detection Service

The following table provides the steps for deploying the Symantec Data Loss Prevention Cloud Detection Service for WSS. Each step is performed by someone with a particular role, as indicated. Before beginning the process, determine who in your organization is responsible for each of the roles.

See "About roles for implementing the Cloud Detection Service for Web Security Services (WSS)" on page 8.

**Table 1-3** Steps for deploying the Cloud Detection Service.

| Step | Action | More information |
|---|---|---|
| 1 | Symantec Data Loss Prevention Administrator:<br><br>Upgrade to Symantec Data Loss Prevention version 15.x if you are running a previous version. | See the *Symantec Data Loss Prevention Upgrade Guide* and *Symantec Data Loss Prevention Administration Guide* for more details. |
| 2 | Network Administrator:<br><br>Open a port for the Enforce Server to communicate with the Cloud Detection Service. | The on-premises Enforce Server must be able to communicate with the cloud detector service using TLS. Your corporate network must allow outgoing traffic to port 443. Make sure that outbound communication from your Enforce Server to port 443 on the internet is open. |
| 3 | Symantec Data Loss Prevention Administrator: | Click the link in your welcome email to log on to the Symantec Data Loss Prevention Cloud Management Portal. |
| 4 | Symantec Data Loss Prevention Administrator:<br><br>Save the enrollment bundle to a directory on the Enforce Server. | After you choose your service in the Cloud Management Portal, Symantec provisions your service in the cloud and sends your organization an enrollment bundle. The bundle is in the form of a ZIP file. This bundle configures your on-premises Enforce Server so that it can connect to your Symantec Data Loss Prevention Cloud Detection Service in the Symantec cloud.<br><br>**Note:** Do not extract the ZIP file. The Enforce Server requires an enrollment bundle ZIP file; extracted files in XML format do not work.<br><br>See "Saving the enrollment bundle" on page 13. |
| 5 | Symantec Data Loss Prevention Administrator:<br><br>Register the Cloud Detection Service cloud detector. | Register the Cloud Detection Service cloud detector on the **Servers and Detectors** page of the Enforce Server administration console. See "Registering the Cloud Detection Service" on page 14. |
| 6 | Symantec WSS Administrator:<br><br>Configure WSS to send ICAP traffic to the Cloud Detection Service for WSS for inspection. | See "Configuring the Symantec Web Security Service integration with Symantec Data Loss Prevention" on page 16. |
| 7 | Symantec Data Loss Prevention Administrator:<br><br>Apply policies to the Cloud Detection Service for WSS. | You manage Symantec WSS policy group assignments on the **System > Servers and Detectors > Policy Groups** page.<br><br>See the online Help topic Manage and add policy groups for more information. |

**Table 1-3** Steps for deploying the Cloud Detection Service. *(continued)*

| Step | Action | More information |
|---|---|---|
| 8 | DLP Admin:<br>Test the Cloud Detection Service. | Generate an incident against a test policy.<br>See the *Symantec Data Loss Prevention Administration Guide* for more information. |

# Using the Cloud Management Portal

With the Symantec Data Loss Prevention Cloud Services Cloud Management Portal (CMP) you can initiate your cloud services after you purchase them. After you place your order, you'll receive a welcome email from Symantec order processing. This email includes information on how to obtain a Symantec Secure Login account, if you do not already have one. It also contains a link to the Cloud Management Portal.

**To log on to the Cloud Management Portal**

1. Log in to Symantec Secure Login, or create a Symantec Secure Login account.
2. Click the link in the email to reach your Cloud Management Portal account.
3. Log in to your CMP account.
4. On the dashboard, view the cloud services that you have purchased and configure them for your particular email forwarding configuration.

A Symantec Secure Login account is required to complete the registration process and manage your Symantec cloud services.

**To create a Symantec Secure Login account**

1. Check your inbox for the email that was sent from CyberDefense@symantec.com, with the subject line “Welcome to Symantec Security Cloud – Confirm Email Address.” If you do not find the email in your Inbox, check your Junk mail folder.
2. Click the **Confirm** link in this email to establish your Symantec Secure Login account.
3. Go to https://login.symantec.com/ and click **Having Trouble Signing In** if you cannot log on to your Symantec Secure Login account or need to reset your password.
4. If you are not the registered user mentioned in this email, contact a registered user in your company. Any registered user can add you to your corporation’s account as a registered user.

**To initiate your cloud service**

1. Provide an email address or distribution list address (recommended). Symantec cloud services sends the enrollment bundle to this address.
2. If you want to convert an existing Trial service to a Production service, choose the service you want to convert.
3. Click **Convert**.
4. If you are configuring a new Production service, choose a region.

   **Note:** Symantec offers two region choices: North America or Europe. You can choose either region, no matter where you are located. You can choose a different region for each of your cloud services, as long as they are each connected to different Enforce Servers. Each Enforce Server can only connect to one Data Loss Prevention cloud region.

5. Click **Configure**.

After you click **Configure**, Symantec cloud services sends you an enrollment bundle, which you should receive by the end of the next business day.

After you set up a cloud service, you can always come back to your Cloud Services overview page in the CMP to see the configuration status of your services. If you are waiting for your enrollment bundle for a service, the status is **In Progress**.

# Saving the enrollment bundle

After you click **Configure** in the CMP, Symantec sets up your detection service in the cloud and sends you an enrollment bundle by the end of the next business day. This bundle contains the information that you need to set up the connection from your on-premises Enforce Server to the Symantec managed detection service.

You can copy the enrollment bundle to any directory on your Enforce Server. Do not extract the enrollment bundle ZIP file. The Enforce Server administration console needs the enrollment bundle in the form of a ZIP file; extracted XML files do not enable enrollment.

**Note:** The enrollment bundle can be used to register the service only once and expires 10 calendar days after you receive it. For security reasons, you should ensure that no other user can access the bundle. To ensure limited access, change the properties of the destination folder so that no other user can read it or write to it. If you have waited longer than 10 calendar days to save your bundle and register the service, contact Symantec Support for a new enrollment bundle: https://support.symantec.com.

For example, on Windows, save the bundle to `C:\Users\<username>\Downloads` or any other subfolder under `c:\Users\username`. On Linux, save the bundle to`/home/username/` or any subfolder under `/home/username/`.

**Note:** You should receive an enrollment bundle shortly after Symantec provisions your service. If you have not received an enrollment bundle in a reasonable amount of time, check your Junk mailbox. Also, check with your internal IT department to ensure that your company has no inbound filters that may block receipt of the enrollment bundle.

# Registering the Cloud Detection Service

After you save the enrollment bundle, you can register your detector, enabling your on-premises Enforce Server to communicate with the Symantec Data Loss Prevention Cloud Detection Service for WSS cloud detector.

**To add a Cloud Detection Service cloud detector**

1. Log on to the Enforce Server as Administrator.
2. Go to **System > Servers and Detectors**.

   The **Overview** page appears.
3. Click **Add Cloud Detector**.

   The **Add Cloud Detector** screen appears.
4. Click **Browse** in the **Enrollment Bundle File** field.
5. Locate the `enrollmentbundle.zip` that you received from Symantec and saved to your Enforce Server.

   The detector description for the chosen enrollment bundle appears. Verify that you have chosen the Cloud Detection Service bundle.
6. Add a name for this detector in the **Detector Name** field.
7. Click **Enroll Detector** to enroll your Symantec Data Loss Prevention Cloud Detection Service cloud detector. The enrollment process can take some time. You can track its progress on the **Servers and Detectors > Overview** page.

It may take several minutes or longer for the Enforce Server administration console to show a **Connected** status for the Cloud Detection Service cloud detector. To verify that the service was added, return to the **Servers and Detectors > Overview** page. Verify that the Cloud Detection Service appears in the list, and that the status indicates **Connected**.

After you have deployed and configured your Symantec Data Loss Prevention Cloud Detection Service, you can apply policy groups on the **System > Servers and Detectors > Policy Groups** page in the Enforce Server administration console.

Chapter 2

# Integrating the Symantec Web Security Service with Symantec Data Loss Prevention

This chapter includes the following topics:



## About integrating the Symantec Web Security Service with Symantec Data Loss Prevention

You can configure the Symantec Web Security Service (WSS) to direct requests to the Cloud Detection Service to inspect HTTP and HTTPS traffic for sensitive data. Symantec Data Loss Prevention scans your employee outbound traffic using Symantec Data Loss Prevention policies and returns information about policy violation to WSS. WSS then blocks user actions that violate your policies.

The following response rules apply to WSS incidents:

- **All: Add Note**
- **All: Limit Incident Data Retention**
- **All: Log to a Syslog Server**

- **All: Send Email Notification**
- **All: Set Attribute**
- **All: Set Status**
- **Network Prevent: Block HTTP/S**
- **Network Prevent: Remove HTTP/S Content**
- **Network Prevent: Block FTP Request**

You can find information about response rules in the section titled "Responding to policy violations" in the *Symantec Data Loss Prevention Administration Guide*.

For more information about integrating the Symantec Web Security Service with Symantec Data Loss Prevention, see the Symantec Web Security Service documentation here: http://portal.threatpulse.com/docs/sol/Solutions/ManageDLP/SYMDLP/symdlp_co.htm.

# Configuring the Symantec Web Security Service integration with Symantec Data Loss Prevention

The latest procedures for integrating Symantec Data Loss Prevention with Symantec WSS are available here: http://portal.threatpulse.com/docs/sol/Solutions/ManageDLP/SYMDLP/symdlp_int.htm. You must register the Cloud Detection Service for WSS before following these procedures.

See “Registering the Cloud Detection Service” on page 14.

By default, the Web Security Service scans requests for all content requesting sources (Deployment Types, Allowed and Trusted Sources, and Users and Groups). You can limit what sources are subject to Symantec Data Loss Prevention scanning.

# Working with Symantec Web Security Services incidents

You manage Symantec WSS policy group assignments on the **System > Servers and Detectors > Policy Groups** page. See the online Help topic Manage and add policy groups for more information.

Policy violations identified through the Symantec Data Loss Prevention integration with Symantec WSS appear as **Incidents > Network** incident reports in the Enforce Server administration console. See the online Help topic Network incident list for more information.

For details about the available response rules and steps to configure response rule actions, see "Response rules for the Cloud Applications and API Appliance detectors" in the chapter

"Responding to policy violations" in the *Symantec Data Loss Prevention Administration Guide* at https://www.symantec.com/docs/DOC9261.

When WSS blocks a user action based on a Symantec Data Loss Prevention policy violation, the user does not receive any information about why the action was blocked. You can view all of the details about the incident in the Enforce Server administration console.

---

**Note:** The default minimum detection threshold for the Symantec Data Loss Prevention Cloud Detection Service for Web Security Service (WSS) is 4 KB (4096 bytes). ICAP traffic that falls under this threshold is not submitted for detection. If your organization has a significant amount of traffic that falls below the default detection threshold, it can be reduced by Symantec Enterprise Technical Support. Contact Symantec Enterprise Technical Support at https://support.symantec.com.

---

Chapter 3

# Migrating from the REST Cloud Detection Service to the Cloud Detection Service for WSS

This chapter includes the following topics:



## About migrating from your existing Cloud Detection Service to the new Cloud Detection Service for WSS

In previous releases, Symantec enabled you to integrate Symantec Data Loss Prevention with Symantec WSS using the REST-based Cloud Detection Service. Support for Symantec WSS using the REST-based Cloud Detection Service will be removed in a future Symantec Data Loss Prevention release. Symantec recommends migrating to the new Cloud Detection Service for WSS for all users of Symantec Data Loss Prevention 15.x.

You can migrate to the new Cloud Detection Service for WSS following this procedure:

**To migrate from your existing Cloud Detection Service to the new Cloud Detection Service for WSS**

1. If you have not already done so, upgrade your Symantec Data Loss Prevention deployment to version 15.x.
2. Contact Symantec Data Loss Prevention Symantec Support to request WSS integration with the new Cloud Detection Service for WSS.

   Your existing integration will remain active during the provisioning process of the new Cloud Detection Service for WSS.
3. Symantec provisions the new Cloud Detection Service for WSS. No action is required on your part for this step.
4. When the provisioning process is complete, Symantec sends you a new Cloud Detection Service for WSS enrollment bundle. This bundle includes the Cloud Detection Service for WSS cloud detector URL and ID.

   See "Saving the enrollment bundle" on page 13.
5. After you have saved the enrollment bundle, register the Cloud Detection Service for WSS in the Enforce Server administration console.

   See "Registering the Cloud Detection Service" on page 14.
6. Work with your Symantec WSS administrator to direct content for inspection to the Cloud Detection Service for WSS. In the Symantec WSS management portal, enter the Cloud Detection Service for WSS cloud detector URL and ID.

   For more information about configuring the Symantec Web Security Service integration with Symantec Data Loss Prevention, see http://portal.threatpulse.com/docs/sol/Solutions/ManageDLP/SYMDLP/symdlp_int.htm.
7. Confirm your migration with Symantec Support.
8. If you are using the REST-based Cloud Detection Service to integrate with Symantec CloudSOC or a third-party cloud application, Symantec will keep your REST-based cloud detector in service. Otherwise, the REST-based cloud detector will be removed.

## Verifying the Cloud Detection Service version in the Enforce Server administration console

You can verify the version of your Cloud Detection Service on the **System > Servers and Detectors > Overview** page. Look for the detector name and type in the **Servers and Detectors** section.