

# Symantec MessageLabs Instant Messaging Security.cloud

## Microsoft Office Communications Server and Lync Server Support

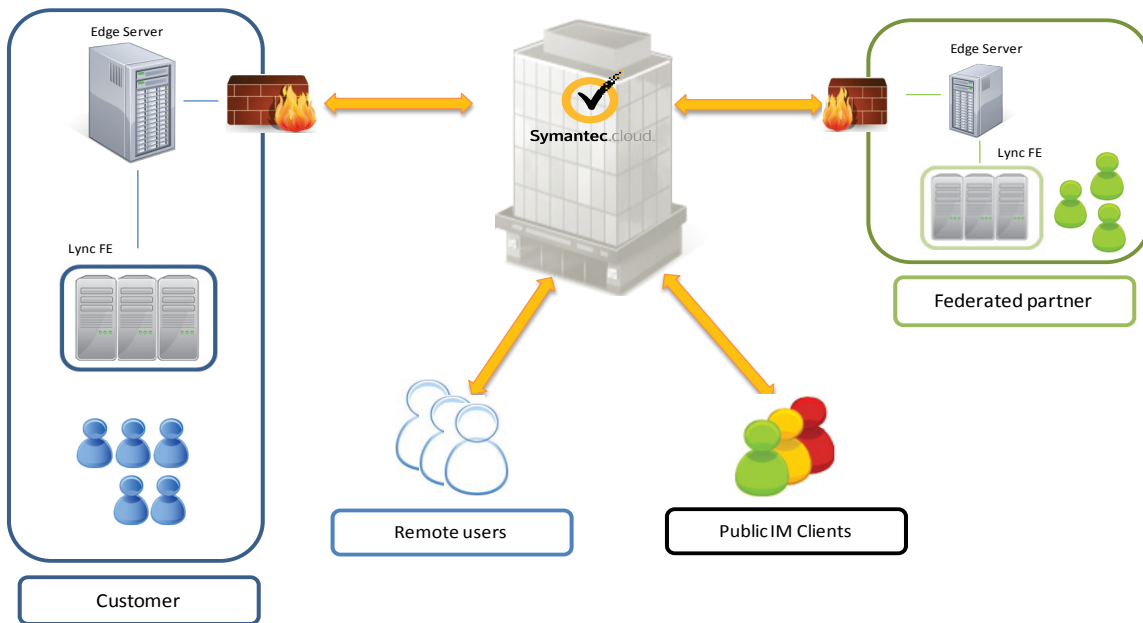
### Can you harness Unified Communications and Instant Messaging's benefits - but avoid its dangers?

MessageLabs Instant Messaging Security.cloud helps companies that communicate externally using Unified Communications and Instant Messaging platforms to meet the challenges of compliance and network security. It scans messages and attachment for malware, blocks malicious URL links, helps protect against data loss and logs messages to aid with compliance.

As a cloud based service, there is no hardware and minimal software enabling rapid deployment and low ongoing maintenance. Administration is via an easy to use Web-based portal where acceptable use policies can be created at group or individual user level and a wide range of reporting features are available.

MessageLabs Instant Messaging Security.cloud provides a comprehensive, cost-effective suite of leading-edge capabilities which help to maximize the return on investment of Microsoft Office Communications Server and Lync Server deployments by providing security and control for external communications. The service also provides integration with selected Public IM services.

### IMS.cloud for Microsoft OCS and Lync - service overview diagram



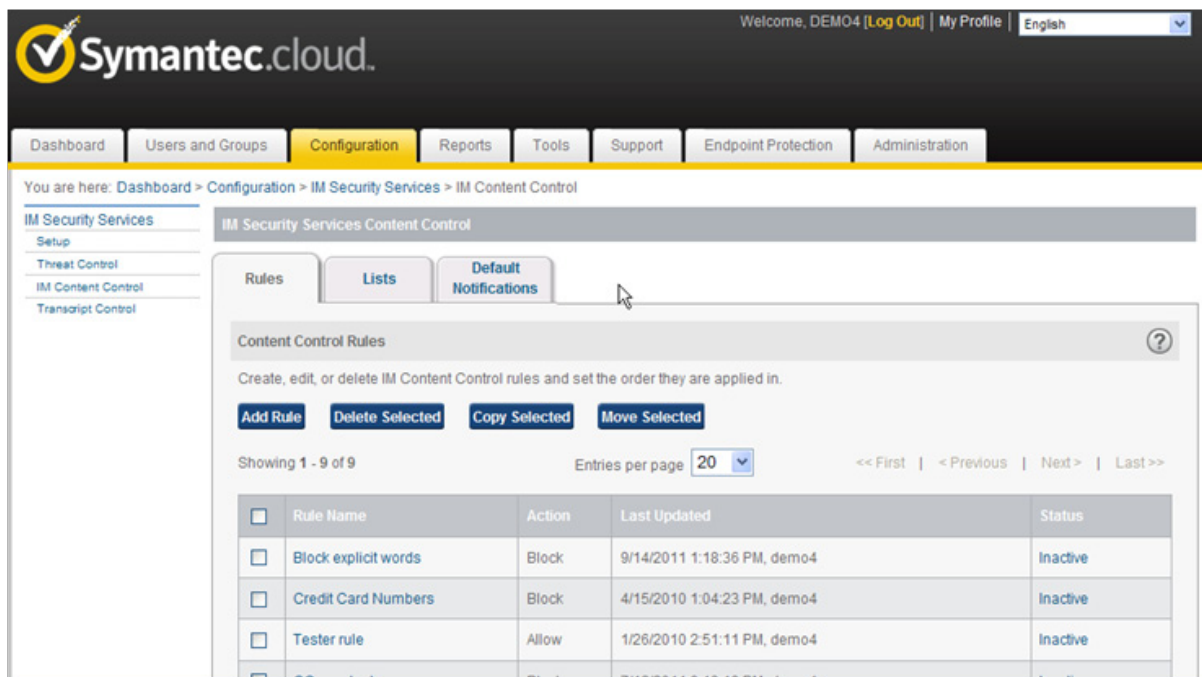
### Key Features and Benefits

<b>Content Control &amp; Disclaimers</b>	Allows rapid creation of an AUP governing UC and IM use at group or individual user level to assist IT with enforcing appropriate use of messaging systems to reduce data loss.
<b>Message Logging and optional archiving</b>	Helps meet regulatory compliance by logging transcripts of messages. Optional archiving feature with e-Discovery capabilities is available for organizations with more stringent compliance needs.
<b>Malware Protection - Skeptic™</b>	Helps to protect your organization from threats delivered over UC and IM networks by scanning messages and file attachments for malware using our proven Skeptic™ technology.
<b>Malicious URL Filtering</b>	Examines URL links contained in messages and blocks access to the Web site if the link is found to be malicious.
<b>Cloud based solution</b>	No on-premise hardware and minimal software allows rapid deployment and low ongoing maintenance.
<b>Directory Synchronisation</b>	Saves administrator time and resource by enabling group data to be kept up to date easily.
<b>Dashboard, &amp; Reporting</b>	Provides visibility, accountability and confidence in the service's effectiveness.
<b>Integrated messaging security and control</b>	When used with MessageLabs Email Security.cloud and MessageLabs Web Security.cloud services, helps provide protection and control over email, Web and UC/IM communications with easy administration from one portal.

## Service Set up and Configuration

MessageLabs Instant Messaging Security.cloud is a cloud based service that is quick and easy to install and requires minimal ongoing maintenance. The following is an overview of the main steps typically required to set up and deploy the service, the actual set up process will depend on each customer's configuration.

### IMS.cloud for Microsoft OCS and Lync - ClientNet Management Portal



### Initial configuration

Log into the management portal ClientNet using the credentials provided by Symantec.cloud. Under "IM Routes", enter the start and end IP ranges of your Lync edge servers, one for each instance. Firewall block rules also need to be in place to ensure that connections to and from edge servers only come via Symantec.cloud IP ranges.

### Setting up Federated domains

Each Federated partner is added to the 'allow' list in the Lync 2010 control panel, just as if IMS.cloud were not present. In the Lync Command Shell enter a command containing the Outbound FQDN supplied by the Symantec.cloud provisioning team. A list of Federated partners is sent to Symantec.cloud for provisioning.

### Setting up Roaming Access

To enable roaming users, an SRV record is created that points to the Roaming FQDN which will have been provided to you by Symantec.cloud.

### Securing Public IM traffic

If you wish to configure IMS.cloud to secure Public IM traffic, your PIC provisioning can be completed according to the instructions provided by Microsoft. Where the Microsoft documentation references the "Access Edge service fully qualified domain name" you will substitute the Inbound FQDN supplied by Symantec.cloud.

### Configuring the IMS.cloud service features

Once you have established connectivity to IMS.cloud from your network, log into the management portal ClientNet and configure the features of IMS.cloud (threat control, content control rules, disclaimers, users and groups, logging and reporting) to suit your organization.

### Supported Platforms

- Microsoft Office Communications Server 2007R2
- Microsoft Lync Server 2010
- Microsoft Windows Live Messenger
- Yahoo! Messenger
- AOL IM 5.9