

---

# Postini Perimeter Manager for Instant Messaging

## User's Guide

**Note to Administrators:** This document helps your IM users with the registration process and provides information about the Perimeter Manager for Instant Messaging service. Please customize this document before distributing to users by replacing any text in the "Red\_Font" style (these are variables that you must change manually).

This document is available in Microsoft Word (for customization) and PDF. Be sure you are using the latest version of this document, which is available on the Postini Support Portal:

<http://support.postini.com>

***To maintain confidentiality, do not distribute this document outside of your organization.***



# Table of Contents

---

Table of Contents .....	2
Introduction .....	3
How to Register for Perimeter Manager for IM.....	6
You will receive the following response from Postini IM Manager: .....	7
Messaging with Perimeter Manager for IM.....	10
AOL Instant Messenger .....	10
Using AOL Instant Messenger .....	10
Receiving Messages .....	10
Sending Messages.....	10
Known Issues .....	10
Windows Live Messenger and MSN Messenger .....	11
Using Windows Live Messenger and MSN Messenger .....	11
Receiving Messages .....	11
Sending Messages.....	11
Features Not Currently Allowed .....	11
Known Issues .....	11
Windows Messenger.....	12
Using Windows Messenger.....	12
Receiving Messages .....	12
Sending Messages.....	12
Known Issues .....	12
Yahoo! Messenger .....	13
Using Yahoo! Messenger .....	13
Receiving Messages .....	13
Sending Messages.....	13
Features Not Currently Allowed .....	13
Known Issues .....	13
Google Talk.....	14
Using Google Talk.....	14
Receiving Messages .....	14
Sending Messages.....	14
Features Not Currently Allowed .....	14

# Introduction

---

## What is Postini Perimeter Manager for Instant Messaging?

---

Postini Perimeter Manager for Instant Messaging helps protect your computer and the company as a whole from unwanted and malicious instant messaging (IM) content. IM has become a valuable tool for business communications, but as the use of IM continues to grow there's an increased risk of malware infection (IM worms and viruses), spim (IM spam), and other security threats.

This service provides protection for instant messaging by:

- Blocking IM worms and viruses
- Filtering incoming IM messages for spim
- Filtering message content based on your company's messaging policies
- Allowing or disallowing file transfers based on your company's messaging policies
- Blocking IM file transfers that contain viruses

## How does this affect me?

---

Once Perimeter Manager for IM is activated, you'll be prompted to register your screen name while using your IM client. For details, see the next section, "How to Register for Perimeter Manager for IM".

To connect to IM at work, you must be a registered user. Your buddies and contacts don't need to be registered to send instant messages to you.

## What happens to my IM conversations?

---

Once you're registered, you'll send and receive messages as usual. If malware or unwanted content is detected during your IM conversations, those messages will be blocked.

Features that have an increased security risk, such as receiving a file by IM, may be unavailable. For more information, please see the section, "Messaging with Perimeter Manager for IM."

## What is our IM messaging policy?

---

<<Optional: Add a reference to your company's messaging policy. >>

## When will Perimeter Manager for IM be activated?

---

<<Optional: Include the date that you plan to activate Perimeter Manager for IM. >>  
Following activation, you'll register to continue using IM. For registration steps, see "How to Register for Perimeter Manager for IM."

## Who should I contact if I have questions regarding IM?

---

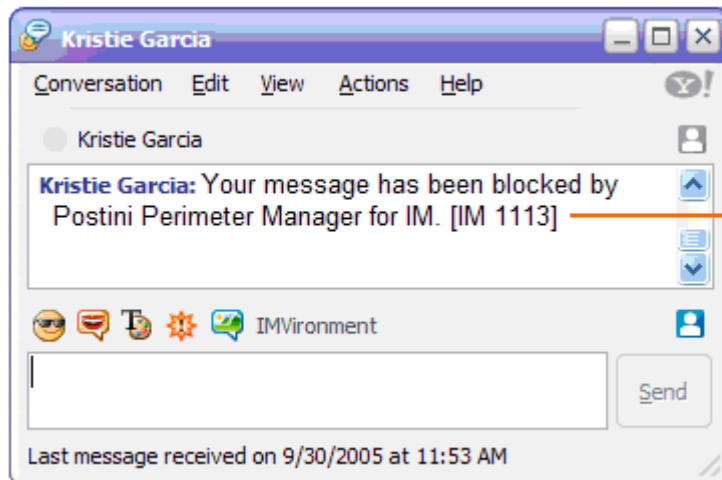
<<Optional: Include contact information at your company for users who have questions.>>

## How will I know when instant messages are filtered?

---

If no malware or unwanted content is detected during your IM conversations, there is no difference in the functioning of your IM client. You'll send and receive messages as usual.

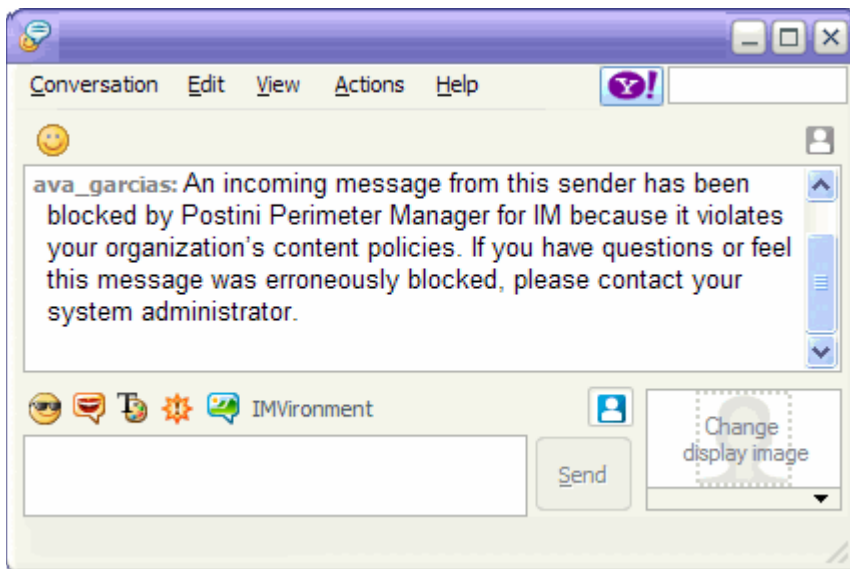
When a user attempts to send you malware or spam, the message is blocked. The sender is sent an IM that their message was blocked:



When a user sends you spam, they receive this message.

When a message from a user outside your organization is blocked, you don't receive any notification in your IM client. However, your administrators can view reports that display statistics on such attempts.

If a message violates the organization's content policy, you'll receive the following response:



### **Can I transfer files using my IM client?**

---

If you use AOL Instant Messenger 5.9, MSN Messenger 7.5, or Windows Live Messenger 8.0, you can send and receive IM file transfers if your company policy allows it. At this time, Postini Perimeter Manager for IM does not allow file transfers sent with Yahoo! Messenger and Google Talk. As an alternative, you can send files as email attachments.

### **Which IM clients are supported by Perimeter Manager for IM?**

---

Perimeter Manager for IM supports and protects the following IM client versions on Windows 2000 or later:

- AOL Instant Messenger 5.9
- Google Talk
- Windows Live Messenger 8.0
- MSN Messenger 7.5
- Windows Messenger 5.1
- Yahoo! Messenger 7.0, 8.0, and 8.1

Please check with your system administrator to confirm which IM clients are approved for use.

### **Does Perimeter Manager for IM support inter-chat between IM protocols?**

---

Inter-chat is currently supported only between Yahoo Messenger 8.0 and MSN / Windows Live Messenger. Inter-chat is *not* supported for earlier versions of Yahoo Messenger.

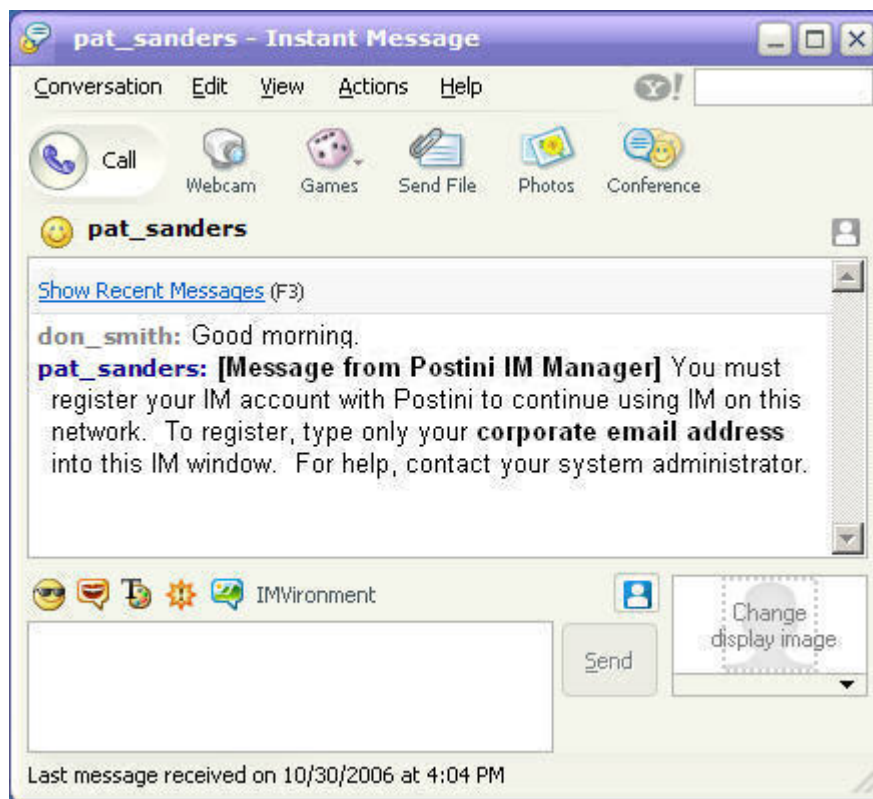
## How to Register for Perimeter Manager for IM

Once Perimeter Manager for IM is activated, you can start the self-registration process. You must participate in this process to continue using IM. Follow these steps:

1. **Log in to your IM client.**
2. **Initiate a conversation with one of your IM buddies.**

The self-registration process begins when you initiate a conversation with one of your IM buddies, or when an IM buddy initiates a conversation with you.

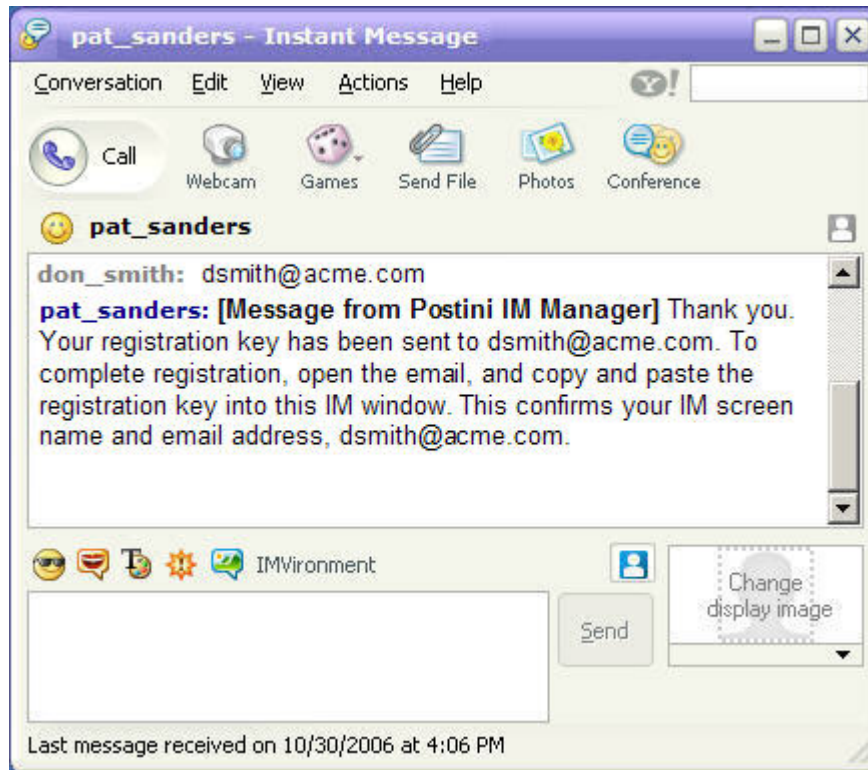
In the example below, an unregistered IM user named Don Smith initiates a conversation with Pat Sanders. Don writes, "Good morning," then receives the following automated message from Postini IM Manager:



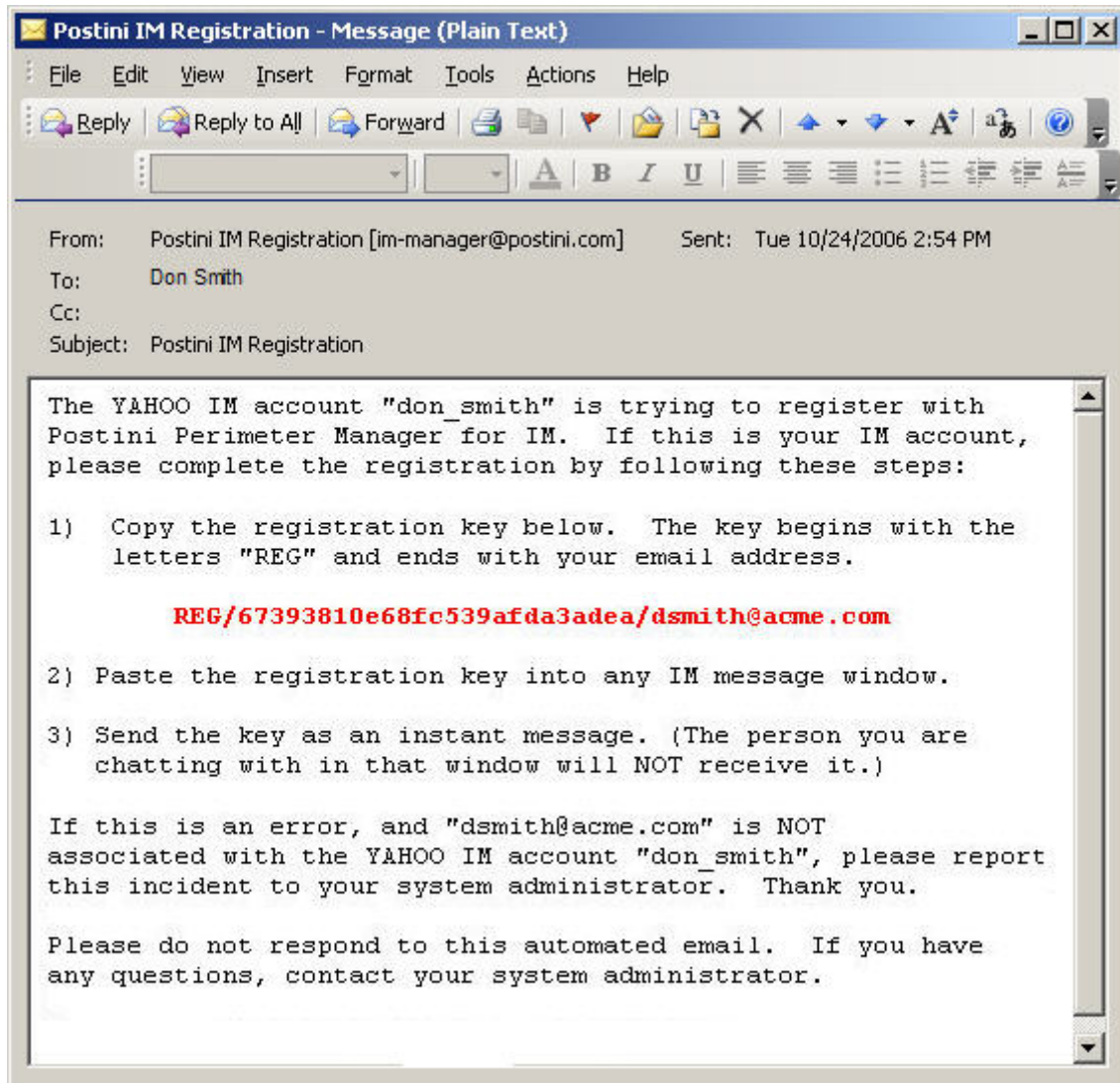
**Note:** You may exchange messages with your buddy for a short grace period until self-registration is completed, but messages from Postini IM Manager will continue to prompt you until you complete the self-registration process.

3. Type your corporate email address into the IM window (for example, dsmith@acme.com) and send the message.

You will receive the following response from Postini IM Manager:

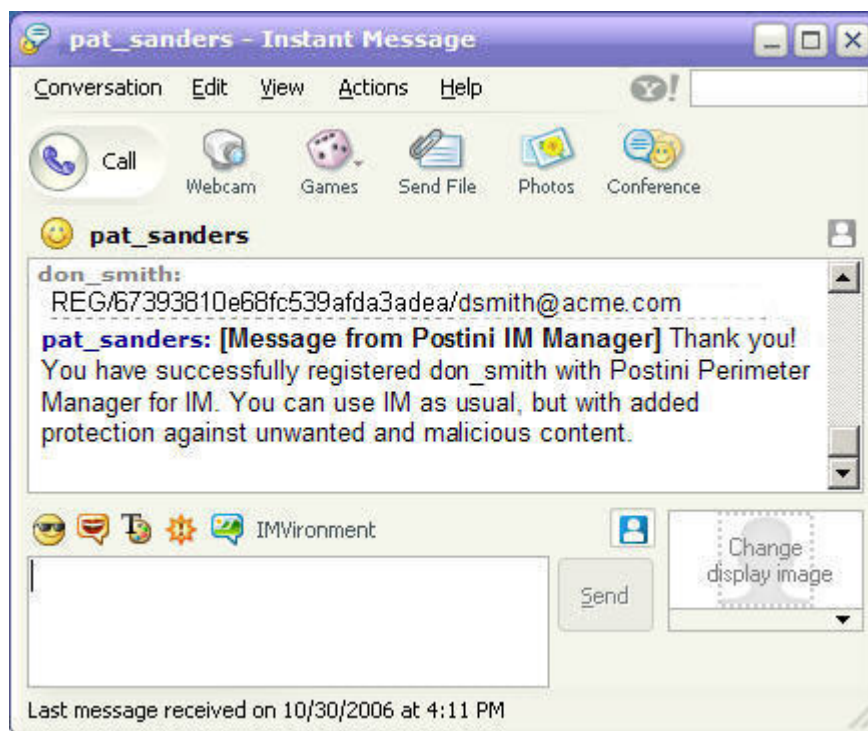


4. Check your corporate email for a message from "Postini IM Registration". Open the message and find the registration key (shown in red in this example):



5. **Copy and paste your registration key into the message window, and send the key as an IM message. Neither the key, nor the address entered in step 3, will be seen by your buddy.**

Once you enter the correct key, you will receive the following message from Postini IM Manager to confirm that you have successfully registered:



**Note:** Self-registration keys expire after five days. Once the original key expires, a new key is sent to you if you try to register using the expired key.

If you aren't sure of any of the steps in the self-registration process, or if you make a mistake, follow the system prompts to help guide you through the process. You must finish the registration process to continue using IM.

# Messaging with Perimeter Manager for IM

---

Perimeter Manager for IM controls certain features in AOL Instant Messenger, Google Talk, Windows Live Messenger, MSN Messenger, Windows Messenger, and Yahoo! Messenger. This section describes the behavior of the various features in these IM clients when Perimeter Manager for IM is activated.

---

## AOL Instant Messenger

Perimeter Manager for IM provides access control, filtering, and content protection for the following AOL Instant Messenger features:

### Using AOL Instant Messenger

- You must be a Perimeter Manager for IM registered user to use AOL Messenger. Your administrator may have registered you, or you can register yourself (see “How to Register for Perimeter Manager for IM”).
- Your IM buddies don’t have to be registered users to send or receive messages from you.

### Receiving Messages

- Messages sent to you are filtered for malicious or unwanted content such as spim (IM spam) or malware (IM worms and viruses).
- If the message contains content that your organization doesn’t allow, the message will be blocked.

### Sending Messages

- Messages you send are filtered for malicious or unwanted content.
- If the message contains content that your organization doesn’t allow, the message will be blocked.

### Known Issues

The following known issues may affect AOL Instant Messenger. These are currently being investigated and will be addressed in a future release:

- Blocking Directory Transfer works, but no error messages are currently displayed for senders or intended recipients.
- When message content is filtered during an IM conference, some participants in the conversation may receive error messages from Postini that they shouldn’t receive.
- In a chat room, users who receive an instant message successfully may sometimes receive an error message that the same message was blocked. Message recipients in a chat room may see multiple blocked messages from Postini.

---

## Windows Live Messenger and MSN Messenger

Perimeter Manager for IM provides access control, filtering, and content protection for the following Windows Live Messenger and MSN Messenger features:

### Using Windows Live Messenger and MSN Messenger

- You must be a Perimeter Manager for IM registered user to use Windows Live or MSN Messenger. Your administrator may have registered you, or you can register yourself (see “How to Register for Perimeter Manager for IM”).
- Your IM contacts do not have to be registered users to send or receive messages from you.

### Receiving Messages

- Messages sent to you are filtered for malicious or unwanted content such as spim (IM spam) or malware (IM worms and viruses).
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Sending Messages

- Messages you send are filtered for malicious or unwanted content.
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Features Not Currently Allowed

Perimeter Manager for IM does not currently allow the following features in Windows Live Messenger and MSN Messenger:

- File sharing

### Known Issues

The following known issues may affect Windows Live Messenger or MSN Messenger. These are currently being investigated and will be addressed in a future release:

- In a chat room, users who receive an instant message successfully may sometimes receive an error message that the same message was blocked. Message recipients in a chat room may see multiple blocked messages from Postini.
- Windows Live Messenger users and MSN Messenger users cannot conduct file transfers with a user using an older version of *Windows Messenger*.

---

## Windows Messenger

Perimeter Manager for IM provides access control, filtering, and content protection for the following Windows Messenger features:

### Using Windows Messenger

- You must be a Perimeter Manager for IM registered user to use Windows Messenger. Your administrator may have registered you, or you can register yourself (see “How to Register for Perimeter Manager for IM”).
- Your IM contacts do not have to be registered users to send or receive messages from you.

### Receiving Messages

- Messages sent to you are filtered for malicious or unwanted content such as spim (IM spam) or malware (IM worms and viruses).
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Sending Messages

- Messages you send are filtered for malicious or unwanted content.
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Known Issues

The following known issues may affect Windows Messenger. These are currently being investigated and will be addressed in a future release:

- File transfers are possible via the Remote Assistance send-file option.
- Windows Live Messenger users and MSN Messenger users cannot conduct file transfers with a user using an older version of *Windows Messenger*.

---

## Yahoo! Messenger

Perimeter Manager for IM provides access control, filtering, and content protection for the following Yahoo! Messenger features:

### Using Yahoo! Messenger

- You must be a Perimeter Manager for IM registered user to use Yahoo! Messenger. Your administrator may have registered you, or you can register yourself (see “How to Register for Perimeter Manager for IM”).
- Your IM contacts do not have to be registered users to send or receive messages from you.

### Receiving Messages

- Messages sent to you are filtered for malicious or unwanted content such as spim (IM spam) or malware (IM worms and viruses).
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Sending Messages

- Messages you send are filtered for malicious or unwanted content.
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Features Not Currently Allowed

Perimeter Manager for IM does not currently allow the following features in Yahoo! Messenger:

- Sending and receiving a file
- Shared files

### Known Issues

The following known issues may affect Yahoo! Messenger. These are currently being investigated and will be addressed in a future release:

- When message content is filtered during an IM conference, some participants in the conversation may receive error messages from Postini that they shouldn't receive.
- If an IM user is part of an organization where external communication is disallowed, and that user joins a conference with participants in another organization, error messages will interrupt the conversation. Users should close the conference and restart it.
- Yahoo voice conferences may fail.

---

## Google Talk

Perimeter Manager for IM provides access control, filtering, and content protection for the following Google Talk features:

### Using Google Talk

- You must be a Perimeter Manager for IM registered user to use Google Talk. Your administrator may have registered you, or you can register yourself (see “How to Register for Perimeter Manager for IM”).
- Your IM contacts do not have to be registered users to send or receive messages from you.

### Receiving Messages

- Messages sent to you are filtered for malicious or unwanted content such as spim (IM spam) or malware (IM worms and viruses).
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Sending Messages

- Messages you send are filtered for malicious or unwanted content.
- If the message contains content that your organization doesn't allow, the message will be blocked.

### Features Not Currently Allowed

Perimeter Manager for IM does not currently allow the following features in Google Talk:

- Sending and receiving a file