

IronPort Plug-in for Outlook
VERSION 1.8
ADMINISTRATOR GUIDE



COPYRIGHT

Copyright © 2007 by IronPort Systems® Inc. All rights reserved.

Part Number: 421-0065B

Revision Date: October 23, 2007

The IronPort logo, IronPort Systems, Messaging Gateway, Virtual Gateway, SenderBase, Mail Flow Monitor, Virus Outbreak Filters, Context Adaptive Scanning Engine (CASE), IronPort Anti-Spam, and AsyncOS are all trademarks or registered trademarks of IronPort Systems, Inc. Brightmail, the Brightmail logo, BLOC, BrightSig, and Probe Network are trademarks or registered trademarks of Symantec Incorporated. All other trademarks, service marks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.

This publication and the information contained herein is furnished “AS IS” and is subject to change without notice. Publication of this document should not be construed as a commitment by IronPort Systems, Inc. IronPort Systems, Inc., assumes no responsibility or liability for any errors or inaccuracies, makes no warranty of any kind with respect to this publication, and expressly disclaims any and all warranties of merchantability, fitness for particular purposes and non-infringement of third-party rights.

IRONPORT SYSTEMS, INC.

IronPort Systems, Inc.
950 Elm Ave.
San Bruno, CA 94066

CONTACTING IRONPORT CUSTOMER SUPPORT

If you have purchased customer support directly from IronPort Systems, you can request support by phone, email, or online 24 hours a day, 7 days a week. During IronPort office hours (24 hours a day, Monday through Friday, excluding U.S. holidays), an engineer will contact you within an hour of your request. To report a critical issue that requires urgent assistance, contact IronPort immediately using the following information:

U.S. Toll-Free: 1 (877) 641-IRON (4766)

International: www.ironport.com/support/contact_support.html

Support Portal: www.ironport.com/support

If you have purchased support through a reseller or another vendor, contact the reseller or vendor for support of your IronPort products.

Table of Contents

1. IronPort Plug-in for Outlook 1

- IronPort Plug-in for Outlook Overview 2
 - How the Plug-in Works 2
 - Deploying the Plug-in 3
- Configuring the Plug-in to Submit Messages Through a Proxy 4
 - IronPort Plug-in for Outlook Proxy Configuration Settings 4
 - Using the Proxy Configuration Utility 5
- Installing and Uninstalling the Plug-in 6
 - Pre-Installation Notes 6
 - Installing the IronPort Plug-in for Outlook 6
 - Uninstalling the IronPort Plug-in for Outlook 6
- Hiding and Disabling the Plug-in 9
 - Hiding the Plug-in 9
 - Disabling the Plug-in 9
- Troubleshooting 10
 - Error Message When Using the IronPort Plug-in for Outlook 10
 - Error Message When Launching Microsoft Outlook 10
 - Outlook Displays Alerts when Reporting Messages 11
 - Outlook Does Not Properly Report Messages When Using a Proxy Server 11

IronPort Plug-in for Outlook

The IronPort Plug-in for Outlook enables Outlook users to submit feedback to IronPort Systems about unsolicited and unwanted email messages, such as spam, viruses, and phishing messages. IronPort Systems uses this feedback to update its filters to stop unwanted messages from being delivered to your inbox.

You can also report false positives, which are legitimate email messages that are marked as spam, to IronPort Systems by using the **Not Spam** button. Legitimate email messages are often referred to as “ham.” IronPort Systems uses reports about false positives to adjust its spam filters to avoid misclassifying legitimate email in the future.

The plug-in provides a convenient interface that enables you to submit feedback by using toolbar buttons and right-click context menus. When you report a message, a dialog box appears indicating that the message was submitted. The message data that you submit is used by automated systems to improve the IronPort filters. By submitting message data, you help to reduce the volume of unsolicited email in your inbox.

This document contains information about the IronPort Plug-in for Outlook and consists of the following sections:

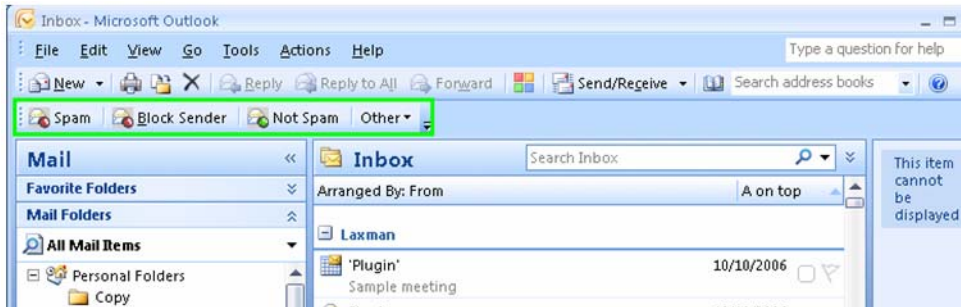
- “IronPort Plug-in for Outlook Overview” on page 2
- “Configuring the Plug-in to Submit Messages Through a Proxy” on page 4
- “Installing and Uninstalling the Plug-in” on page 6
- “Hiding and Disabling the Plug-in” on page 9
- “Troubleshooting” on page 10

You can find additional information in the online help for the plug-in, which you access by clicking Other > Help on the plug-in toolbar.

IRONPORT PLUG-IN FOR OUTLOOK OVERVIEW

The IronPort Plug-in for Outlook provides a toolbar for reporting spam and other email threats. It also provides corresponding items in the right-click menu in Outlook 2003 and 2007. This toolbar contains four buttons: Spam, Block Sender, Not Spam, and Other.

Figure 1-1 IronPort Plug-in for Outlook Toolbar



Use these buttons to report misclassified and harmful email. Misclassified email consists of messages that are erroneously marked as either spam or not spam. Harmful email typically consists of virus and phishing messages. Click **Other > Report threat** on the plug-in toolbar to report harmful mail.

You can report an email message as Spam, Not Spam, or Other. If you choose Other, the threat types are Phish (for phishing messages) and Virus (for virus-infected messages). In addition, you can use the **Block Sender** button to add the sender of a message to the Blocked Senders list in Outlook.

Note — If you select a large number of email messages, or if the messages that you select have a large file size, you might exceed the .pst size limit. When this occurs, Outlook displays an error message. To work around this issue, select fewer messages and attempt to report them again.

How the Plug-in Works

When you report a spam email message to IronPort Systems, the plug-in moves the message from the current mail folder to the Deleted Items folder. When you report a message as Not Spam or Other, the message remains in the current working folder and the plug-in reports the message to IronPort Systems. When you report email messages to IronPort Systems, the feedback reports do not appear in the Sent Items mail folder because the plug-in sends the reports to IronPort using HTTPS. Using HTTPS as a transport mechanism ensures that the data is transferred securely, and it prevents the feedback from being inadvertently blocked if your organization filters outbound email.

The IronPort Plug-in for Outlook creates a mail folder named __IPSpam in the Deleted Items folder. The plug-in creates this folder to queue messages before it submits them to IronPort Systems. Ordinarily, this folder is empty. If you find messages in the folder, the plug-in may

have been unable to submit messages through HTTPS. This occurs when you work offline or if connectivity issues exist. The plug-in attempts to send the messages periodically until connectivity is restored and the messages are successfully delivered.

Deploying the Plug-in

To submit feedback to IronPort Systems through a proxy server, first run the proxy configuration utility (see “Configuring the Plug-in to Submit Messages Through a Proxy” on page 4).

Provide the plug-in setup file and the included .ini file to end users. Instruct users to double-click the setup file and follow the prompts. The .ini file must reside in the same folder as the plug-in setup file.

After the plug-in is installed, end users can click **Other > Help** on the plug-in toolbar to access online help for the plug-in. For troubleshooting information, see “Troubleshooting” on page 10.

CONFIGURING THE PLUG-IN TO SUBMIT MESSAGES THROUGH A PROXY

You can configure the IronPort Plug-in for Outlook to use a proxy server when it submits feedback to IronPort Systems. To configure the plug-in to use a proxy, use the proxy configuration utility, IPConfig.exe.

The proxy configuration utility defines the behavior for all instances of the plug-in in the domain. The proxy settings that you configure are stored in the ComplaintReportPlugin.ini file, which is distributed with the plug-in setup file and the proxy configuration utility. Be sure to include the .ini file with the plug-in setup file when you distribute it to end users.

IronPort Plug-in for Outlook Proxy Configuration Settings

Use the proxy configuration utility to configure the following settings:

Automatic or Manual Proxy Configuration

You can select whether to use a Proxy Auto-Configuration script or specify a proxy URL and port number.

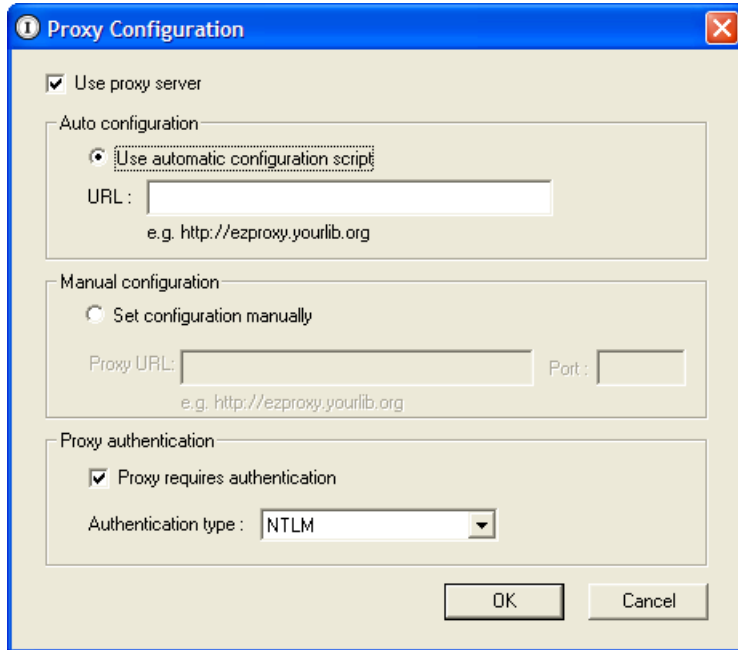
Proxy Authentication

Specify whether or not to use authentication. You can select either basic LDAP authentication or NTLM authentication.

Using the Proxy Configuration Utility

1. Double-click IPConfig.exe to open the proxy configuration utility.

Figure 1-2 Configuring the Plug-in to Use a Proxy Server



2. Select the Use Proxy Server check box. All plug-in instances in the domain use the proxy server.
3. If you have a proxy auto-configuration (PAC) script, select the option for automatic configuration, and enter the URL.

Alternatively, select the option for manual configuration, and enter the URL and port number for the proxy server.

Note — Although some browsers, such as Internet Explorer, do not require server information in URL format, you must specify the server in URL format, regardless of the browser.

4. To enable authentication, select the Proxy Requires Authentication check box, and select an authentication type.
5. Click **OK** to save your changes, or click **Cancel** to close the proxy configuration utility without making any changes.

INSTALLING AND UNINSTALLING THE PLUG-IN

Follow the procedures in this section to install or uninstall the plug-in.

Pre-Installation Notes

Before you install the IronPort Plug-in for Outlook, you must uninstall previous versions of the plug-in. To uninstall previous versions, see “Uninstalling the IronPort Plug-in for Outlook” on page 6.

Installing the IronPort Plug-in for Outlook

To install the IronPort Plug-in for Outlook:

1. Close Microsoft Outlook, if it is running.
2. Save the plug-in setup file and the ComplaintReportPlugin.ini file in the same folder on your hard drive.
3. Double-click the plug-in setup file. The InstallShield wizard opens.
4. Click **Next**.
5. Read and agree to the license agreement.
6. Click **Finish**.

Uninstalling the IronPort Plug-in for Outlook

You can uninstall the IronPort Plug-in for Outlook by using the Control Panel > Add or Remove Programs option or by running the setup program that you used to install the plug-in.

When you uninstall the plug-in, the following items are removed:

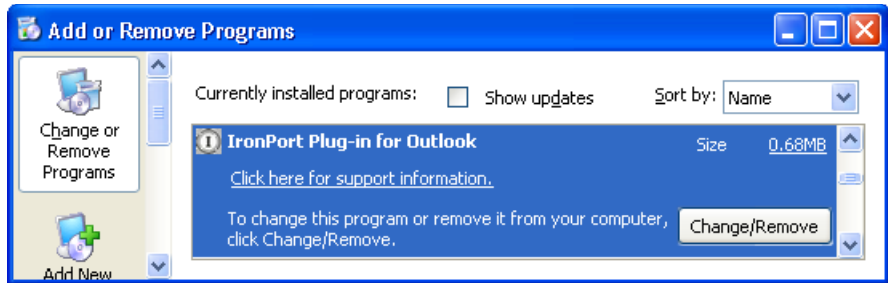
- All registry entries made by the plug-in.
- Entry for the plug-in in the Add/Remove programs listing.
- Files related to the plug-in.

Microsoft Outlook functions normally after you uninstall the plug-in.

To uninstall the plug-in from the Windows Control Panel, complete the following steps:

1. Close Microsoft Outlook if it is running.
2. Click Start > Settings > Control Panel > Add/Remove Programs.
3. Select “IronPort Plug-in for Outlook,” and click **Change/Remove**.

Figure 1-3 Removing the IronPort Plug-in for Outlook



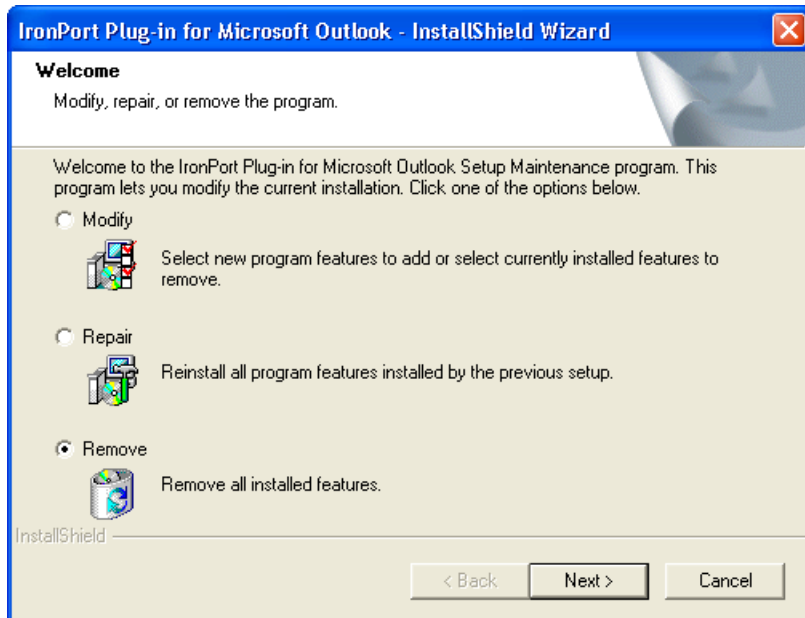
Alternatively, you can use the plug-in setup file to uninstall the plug-in.

To uninstall the plug-in by using the setup file, complete the following steps:

1. Double-click the .exe file that you used to install the plug-in.

The Modify, Repair, or Remove dialog box is displayed.

Figure 1-4 Removing the IronPort Plug-in for Outlook



2. Select the “Remove” option to uninstall the IronPort Plug-in for Outlook.
3. Click **Next**.

4. Click **OK** to confirm, and then click **Finish**.
5. If necessary, delete the __IPspam folder from the Deleted Items folder in Outlook.

HIDING AND DISABLING THE PLUG-IN

You can hide or disable the IronPort Plug-in for Outlook without uninstalling it.

Hiding the Plug-in

You can remove the plug-in toolbar from the Outlook menu bar. To hide the toolbar, click Tools > Customize > Toolbars, and clear the IronPort Plug-in check box. To report a message after you hide the toolbar, right-click the message that you want to report and select the appropriate plug-in option in the context menu.

Disabling the Plug-in

You can disable the plug-in in Outlook 2007 without uninstalling it. To disable the plug-in, complete the following steps:

1. Click Tools > Trust Center > Add-ins.
2. Select "COM Add-ins" from the Manage list, and click Go.
3. Clear the IronPort Plug-in for Outlook check box.

The IronPort Plug-in for Outlook toolbar and context menu options no longer appear in Outlook.

TROUBLESHOOTING

This section describes troubleshooting issues.

Error Message When Using the IronPort Plug-in for Outlook

The following message may appear when you click any of the IronPort Plug-in for Outlook toolbar buttons in Outlook:

Figure 1-5 Non-Email Item Selected Error

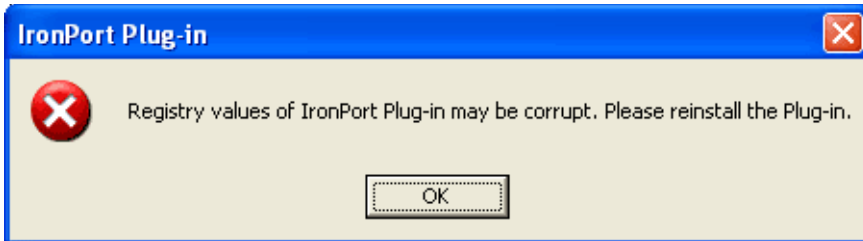


This error message appears if the item selected is a non-email item, such as a meeting request, for example. Click the **OK** button to dismiss the error. Verify that the selected item is an email message.

Error Message When Launching Microsoft Outlook

The following error message may appear when you launch Microsoft Outlook:

Figure 1-6 Registry Values Error



This indicates that certain registry entries associated with the IronPort Plug-in for Outlook are either missing or corrupt. To fix this issue, first close Outlook and then re-run the setup file to either repair or reinstall the plug-in application.

Outlook Displays Alerts when Reporting Messages

When Outlook reports messages, it may display the following security alert:

Figure 1-7 Outlook Security Alert



If this security alert appears, click **Yes** to allow Outlook to report the messages.

Outlook Does Not Properly Report Messages When Using a Proxy Server

If the plug-in does not properly report messages when you use a proxy server, you can test the proxy server. Configure your web browser with the proxy server settings and attempt to connect to the following URL:

<https://ipas-complaints.ironport.com>

To configure the proxy server settings, go to Tools > Internet Options > Connection > LAN settings, and configure the same proxy settings that you used for the IronPort Plug-In for Outlook. If you cannot connect to the site using the proxy server, the issue is with the proxy server or your configured connection to the proxy server.

