



Workshare Ltd. (UK)  
20 Fashion Street  
London  
E1 6PX  
UK

Workshare Inc. (USA)  
208 Utah Street  
350  
San Francisco  
CA 94103  
USA

Workshare Website: <http://www.workshare.com>

## Copyright

© 2008. Workshare Ltd. All rights reserved. Workshare and Workshare Protect are registered trademarks of Workshare Ltd. Workshare DeltaView, Workshare Protect, Workshare Professional, Workshare 3, Workshare DeltaServer, Workshare Synergy, Workshare Synergy Editor, SafetyGain and the Workshare logo are trademarks of Workshare Ltd. PDFNet SDK is a copyright of PDFTron™ Systems, 2001-2006, and distributed by Workshare Ltd. under license. All rights reserved. Outside In® XML Export © 1991-2006 Stellent Chicago, Inc. All rights reserved. All other trademarks are those of their respective holders.

## Disclaimers

The authors/publishers of the Workshare Protect guides and associated help material have used their best efforts to ensure accuracy and effectiveness. Due to the continuing nature of software development, it may be necessary to distribute updated Help from time to time. The authors would like to assure users of their continued best efforts in supplying the most effective Help material possible.

The authors/publishers, however, make no warranty of any kind, expressed or implied, with regard to Workshare programs or Help material associated with it, including this Guide. The authors/publishers shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the programs or associated Help instructions.

## A Note on Trademarks

Trademarked names appear throughout this guide and on other parts of the Workshare CD. Instead of listing these here or inserting numerous trademark symbols, Workshare wishes to state categorically that no infringement of intellectual or other copyright is intended and that trademarks are used only for editorial purposes.

---

# Table of Contents

<b>Chapter 1: Introducing Workshare Protect</b> .....	<b>4</b>
Overview of Outbound Content Security Risks .....	4
Introduction to the Workshare Protect Product Line .....	5
Workshare Protect Premium .....	6
Workshare Policy Designer.....	6
Workshare Policy Manager.....	6
Workshare Protect Network Overview .....	7
Workshare Protect Network Components.....	7
Incident Management Workflow and Self-Review .....	7
Workshare MTA .....	8
BlackBerry Support.....	8
Fingerprinting Service.....	8
Security .....	8
Workshare Network Monitor .....	9
Reporting .....	9
Audit Service.....	10
Workshare Protect Manager.....	10
<b>Chapter 2: Protect Network Manager</b> .....	<b>11</b>
Logging Into the Protect Network Manager.....	11
Sending Feedback .....	15
<b>Chapter 3: Reviewing Emails</b> .....	<b>17</b>
Reviewing Protect Network Notify Emails.....	18
Allowing Emails.....	21
Blocking Emails.....	22
Viewing the Email Contents.....	24
Adding Comments to Email Incidents.....	26
Changing the Email Incident Owner .....	27
Changing the Email Incident Worklist .....	28
Sharing the Email Incident.....	29

---

<b>Appendix E: Customer Support</b> .....	<b>31</b>
Related Technical Documentation .....	31
Workshare Knowledge Base.....	31

---

# Chapter 1: Introducing Workshare Protect

This chapter provides an overview of Workshare Protect, including how it works and a summary of its key features.

This chapter includes the following sections:

Overview of Outbound Content Security Risks .....	4
Introduction to the Workshare Protect Product Line .....	5
Workshare Protect Premium .....	6
Workshare Protect Network Overview .....	7
Workshare Protect Network Components .....	7

## Overview of Outbound Content Security Risks

Companies, government agencies and other organizations invest huge resources developing security policies and procuring protective technologies that point outwards at hackers, spyware, and viruses. However, there is another aspect to content security, the inside-out leakage of information. Not only do organizations need to worry about the release of valuable intellectual property, but they must now also deal with increased regulation and oversight of issues ranging from consumer privacy to financial disclosure.

The inside-out threat poses serious risks that have the capacity to cost companies huge sums in law suits, regulatory penalties, lost business, intellectual property infringement as well as unquantifiable damage to that most valuable of assets - reputation. The release of hidden information in documents by major corporations has led to the release of financial data and company strategy and revealed highly classified government information.

Managing the risks associated with the exchange of business content requires a combination of policy and enforcement. All of these inadvertent disclosures of confidential hidden content could have been avoided if the documents had been cleaned, based on content security polices, before being transmitted outside the company perimeter. Workshare Protect protects organizations from unauthorized content disclosure and ensures document integrity.

---

## Introduction to the Workshare Protect Product Line

The Workshare Protect product line includes both client and network-level outbound content security and compliance solutions to protect organizations from unauthorized content disclosure and ensure document integrity, including protection against loss of confidential information from mobile devices such as laptops, removable storage devices (USB key drives and digital cameras), and PDAs. Workshare Protect delivers a unique combination of integrated approaches to prevent widespread privacy breaches, intellectual property leakage and inadvertent financial disclosures that often result from dirty and dangerous content.

Workshare Protect unifies fragmented approaches to outbound content compliance by converting content risk into safe information and containing sensitive information within established perimeters. This controls confidential content over electronic channels inside or outside your company's perimeter.

The Workshare Protect product line:

- Enforces content security policies at both the network and client level
- Provides protection for information workers using laptops, PDAs, and removable devices
- Provides enterprise-level centralized management, audit and reporting
- Provides robust content filtering techniques for multiple protocols and content types
- Provides always-on risk alerts to policy condition violations
- Utilizes identity-based routing using LDAP integration and auditing to ensure that sensitive content is sent and received by only the appropriate parties with the appropriate cure
- Provides robust client and server-side policy actions such as alerting users to visible and hidden content violations, cleaning documents of content risk, SMTP blocking, converting documents to PDF, encrypting outbound traffic and applying document rights

The Workshare Protect product line includes the following components: Workshare Protect Premium and Standard versions, and Workshare Protect Network. These components can work independently or together to deliver the right solution, at the right time and in the right place without crippling existing business processes.

---

## Workshare Protect Premium

Workshare Protect Premium is the client-level component of the Workshare Protect product line that is seamlessly integrated with Microsoft Office and automatically enforces company security policy at end-user workstations. Working both online and offline, Workshare Protect Premium can be configured to remove content risk, convert content to appropriate formats, and apply content rights. Rather than simply block information flow, Workshare Protect Premium warns and educates users in real-time about sensitive information and, if authorized, lets users decide how to treat the content. Workshare Protect Premium includes the following components:

- Email remediation with block, alert, LightSpeed Clean, PDF and ZIP capabilities
- Active content channel remediation for in-use Microsoft Office documents
- Batch Cleaning to quickly clean sensitive and hidden data from multiple files
- Packaged compliance policies for out of the box enforcement
- Removable device channel remediation for USB drives and more
  - Workshare Protect Premium removable device channel remediation is not compatible with third-party music synchronization applications and their associated devices, including Apple iTunes and iPod. Third-party devices will not be accessible if Workshare Protect Premium removable device channel remediation is installed.
- Policy Designer for centralized policy management
- Policy Manager for fast and easy policy creation
- Optional Workshare Ready! Partner add-ins, including solutions from Cryptzone, Utimaco, PGP, Rpost, and Microsoft RMS

For detailed information about Workshare Protect Premium functionality, refer to the Workshare Protect Premium Administrator's Guide.

## Workshare Policy Designer

The Workshare Protect Policy Designer is a component of Workshare Protect Premium that provides a centralized policy management console for the creation and distribution of policies, enabling you to translate business-driven, company-wide security policies into policy files. Policy files created by the Workshare Protect Policy Designer are easily and automatically distributed to Workshare Protect Premium and Workshare Protect Network end-points.

For detailed information about Workshare Policy Designer functionality, refer to the Workshare Protect Premium Administrator's Guide.

## Workshare Policy Manager

The Workshare Policy Manager is a component of Workshare Protect Premium and Standard versions that provides options to easily configure a global set of Workshare Protect parameters that can be used to standardize the use of Workshare Protect across an organization.

For detailed information about Workshare Protect Premium functionality, refer to the Workshare Protect Premium Administrator's Guide or the Workshare Protect Standard Administrator's Guide.

---

## Workshare Protect Network Overview

Companies, government agencies and other organizations invest huge resources developing security policies and procuring protective technologies that point outwards at hackers, spyware, and viruses. However, there is another aspect to content security: the inside-out leakage of information. Not only do organizations need to worry about the release of valuable intellectual property, but they must now also deal with increased regulation and oversight of issues ranging from consumer privacy to financial disclosure.

Workshare Protect Network is the last line of defense at the network gateway, providing IT security staff with visibility into - and policy enforcement over - content leaving the organization through network channels such as HTTP, SMTP, FTP, IM, and Web mail. By deploying Workshare Protect Network, organizations can audit and control outbound traffic at the network gateway.

Workshare Protect Network monitors over 370 file formats for policy violations, including Microsoft Office documents, emails, PDFs, and hundreds of other common file formats. Workshare Protect Network also monitors HTTP, SMTP, FTP, IM and Webmail channels, including support for the following protocols: Yahoo Mail Classic, MSN Hotmail, AOL Webmail, Gmail, Windows Live Mail, Hotmail via Outlook Express, Windows Messenger, and AOL Instant Messenger.

## Workshare Protect Network Components

### Incident Management Workflow and Self-Review

The incident management workflow automatically handles policy violations based on policies defined in the Workshare Protect Policy Designer. The incident management workflow is integrated with the security, audit, MTA, Network Monitor, policy engine and assets features of the Workshare Protect Network. Policies define which violations become incidents in the system, and which do not. Based on these policies, violations can automatically trigger one or more of the following actions:

- Release: Releases the message to its final destination.
- Escalate: Escalates the incident to configurable recipients, for example, security officers within an organization.
- Bounce: Sends a customized message to the sender, alerting them to the policy violation, and removes the email from the queue.
- Drop: Deletes the message.
- Notify: Sends a notification to the sender and other configurable recipients, and if allowed, provides a link to the violation so the sender can learn about the violation and remediate it.
- Queue: Stores the message in a queue for administrative review or user self-review, if allowed.
- Close: Closes the incident and removes it from the queue.

---

## Workshare MTA

The Workshare MTA (Mail Transfer Agent) inspects outgoing email for policy violations and delivers emails when no violations are found. The Workshare MTA also provides support for email sent from Blackberry PDAs. When an email violates a policy, the appropriate action is taken as dictated by the policy:

- Block: Blocks the email message from being sent.
- Drop: Deletes the message.
- Bounce: Sends a customized message to the sender, alerting them to the policy violation, and removes the email from the queue.
- Notify: Sends a notification to the sender and other configurable recipients, and if allowed, provides a link to the violation so the sender can learn about the violation and remediate it.
- Queue: Stores the message in a queue for administrative review or user self-review, if allowed.
- Add header: Adds a customized MIME header to the subject line of the email and allows it to be sent.
- Create incident: Creates an incident in the workflow.

## BlackBerry Support

The Workshare MTA also inspects email from BlackBerry PDAs, providing visibility into and control over email on the move. Because the Workshare MTA differentiates between regular email traffic and BlackBerry PDA traffic, MTA actions, including block, drop, bounce, notify, queue, add header, and create incident can custom configured for each. For example, attachments sent by regular email may have a “notify” action, whereas attachments sent by BlackBerry may have a “quarantine” action.

## Fingerprinting Service

The fingerprinting service allows documents and document repositories to be manually or automatically added to a blacklist (blocking the content from leaving the network) or a whitelist (allowing content to leave the network). A Web-based UI provides manual whitelist or blacklist registration and inspection of individual documents, while PowerShell cmdlets can be used to instruct the fingerprinting service to automatically crawl and blacklist specified repositories, including Microsoft file shares.

## Security

Access to the components of the Workshare Protect Network is securely controlled by administrator-defined group permissions. Users are manually added to the Workshare Protect Network system, meaning that only users who need access will have it. As an additional layer of security, users have no permissions until they are added to a group. Because permissions are assigned on a group-basis, users inherit the permissions or lack of permissions assigned to their associated group(s). For example, if Sam is added to the HR group, which has read and write permissions, but also to the Everyone group, which has only read permissions, Sam will only have read permissions.

Workshare security permissions include:

- Resource-level: access to existing work lists, reports, folders, and more
- Service-level: creation of work lists, assets, and more

---

## Workshare Network Monitor

The Workshare Network Monitor passively monitors, analyzes, and processes network traffic over HTTP, SMTP, FTP, IM, and Webmail channels to determine if policy violations exist.

The Workshare Network Monitor includes the following components:

- Sniffer: The sniffer captures packets from a network card, reassembles and sorts the packets into a session, and puts it in a queue. The sniffer can be configured to filter traffic over some protocols (for example, only SMTP) or all protocols.
- Protocol analyzer: The protocol analyzer parses UROs (universal request objects) from the items queued by the sniffer and converts them to a standard structure.
- Policy processor: The policy processor processes the parsed information from the protocol analyzer for policy violations.

The Workshare Network Monitor appliance must be deployed with a network switch that supports port mirroring (SPAN) or a network TAP aggregator device (for example, a NetOptics iTAP Port Aggregator).

## Reporting

Reporting provide live data analysis for visibility into network threats.

The reporting Data Explorer provides an instant view into the latest threats, while Web-based reports provide more detailed visibility into threats with the use of custom filters. Reports can be scheduled to run at defined intervals with customized content, and the results can be exported to PDF or scheduled for email delivery. Reports data can be sorted by the following elements:

- Date range
- Egress point
- Policy set
- Policy
- Action
- Risk level
- Channel

---

## Audit Service

The auditing service analyzes data from the Workshare MTA, Workshare Network Monitor, and Workshare Protect, and routes information about policy violations to the reporting service.

## Workshare Protect Manager

The Workshare Protect Manager includes Web and CLI-based management portals that provides access to the following components:

- Reporting
- Audit service
- Policy Manager
- Fingerprinting service
- Workflow management and self-review
- Security for users and groups

---

## Chapter 2: Protect Network Manager

This chapter describes how to log into Workshare Protect Network Manager, the Web-based management interface for Workshare Protect Network.

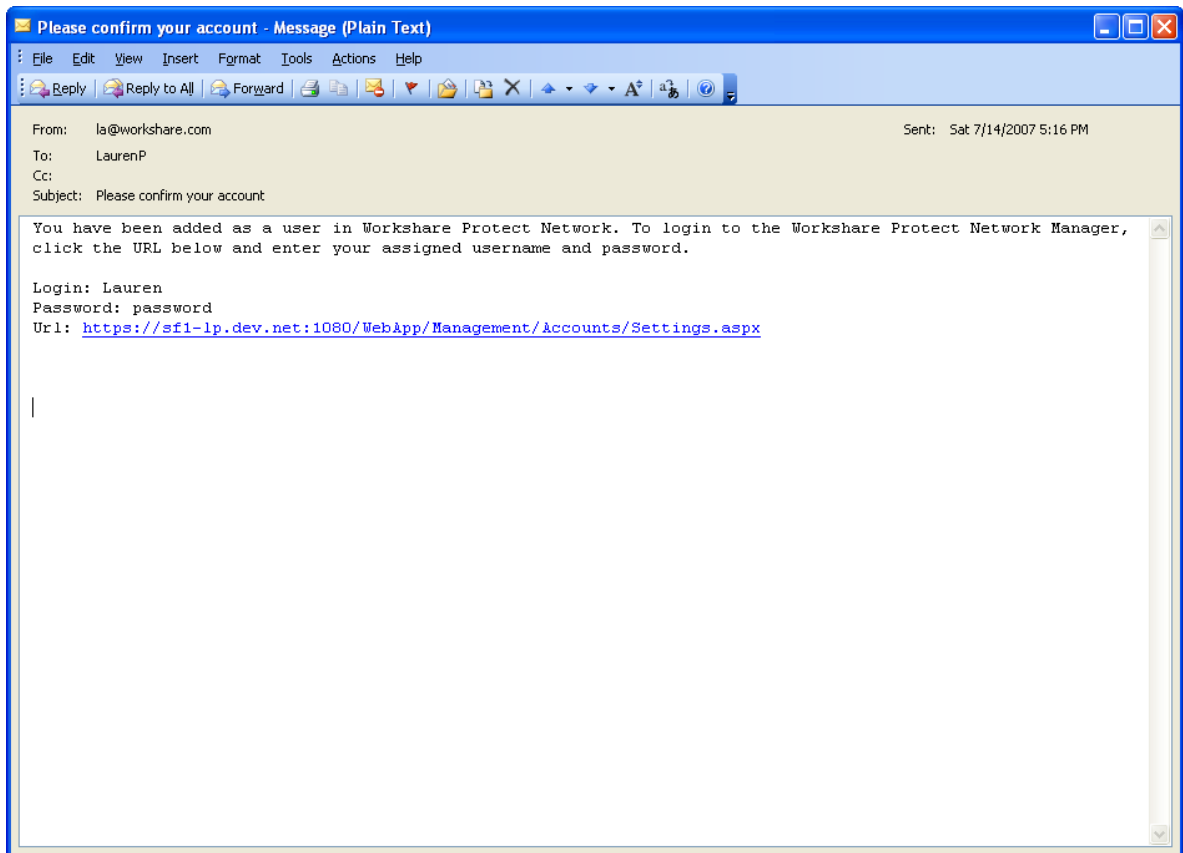
This chapter includes the following sections:

Logging Into the Protect Network Manager.....	11
Sending Feedback.....	15

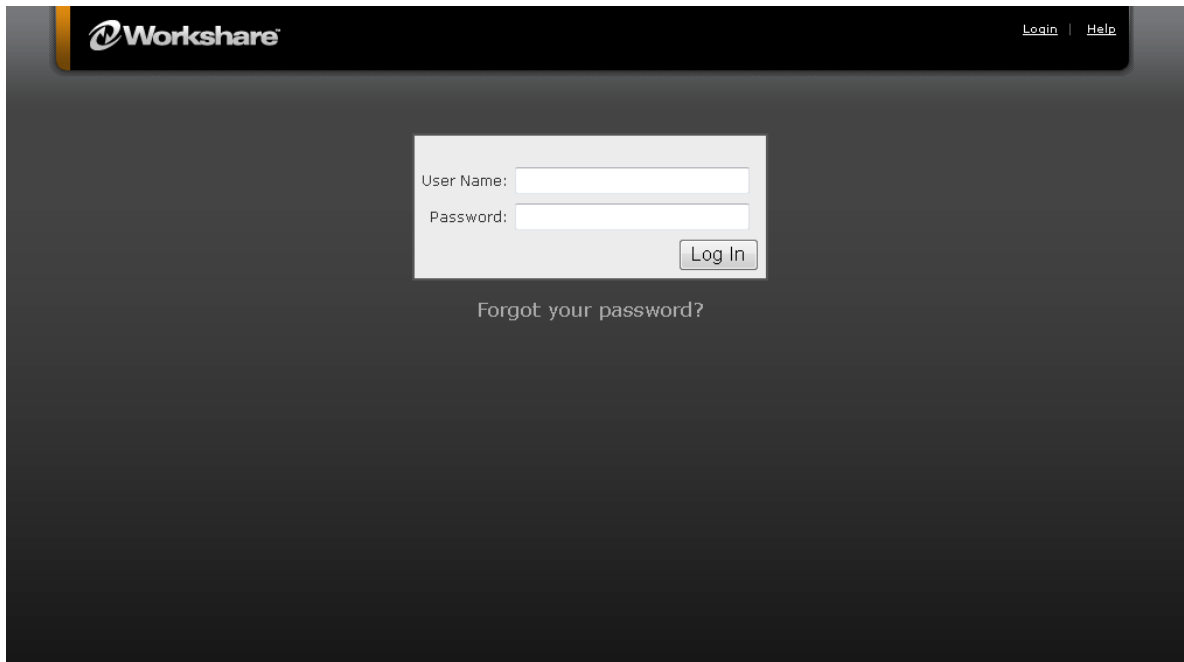
### Logging Into the Protect Network Manager

When your administrator adds you as a user in Workshare Protect Network, you will receive an email notification that includes the URL to the Web-based management interface and your default username and password. To log in, perform the following steps:

1. Click the URL link in the email you receive from your administrator.



2. Type the assigned username and password in the **Username** and **Password** fields and click **Log in**.



Workshare

[Login](#) | [Help](#)

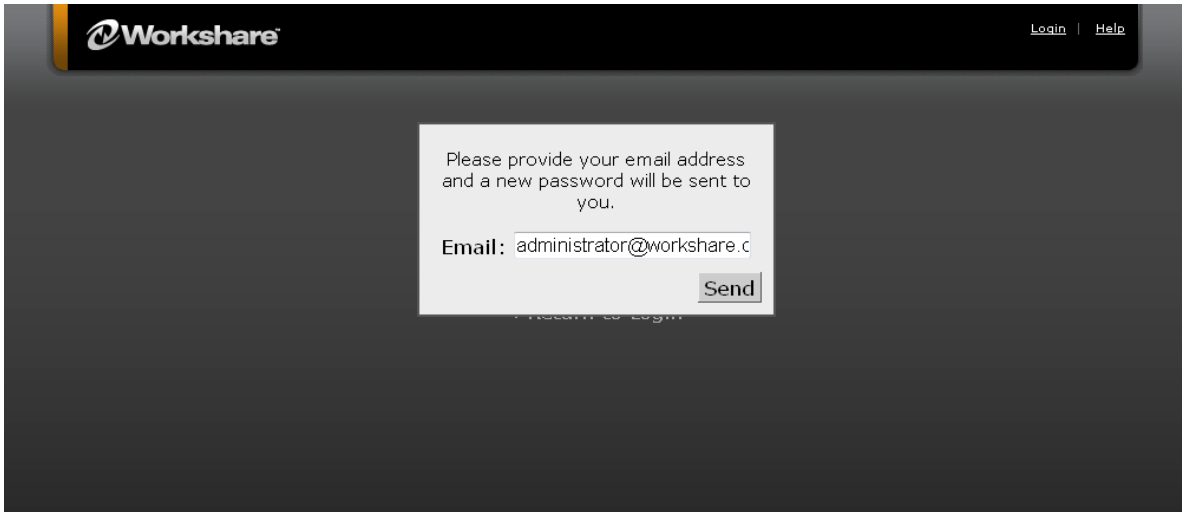
User Name:

Password:

Log In

[Forgot your password?](#)

3. If you need to reset your password, click the **Forgot Your Password** link to have a new password emailed to you.



The screenshot shows a dark-themed web interface for Workshare. At the top left is the Workshare logo, and at the top right are links for "Login" and "Help". In the center, a white box contains the text: "Please provide your email address and a new password will be sent to you." Below this is a text input field with "Email: administrator@workshare.c" and a "Send" button.

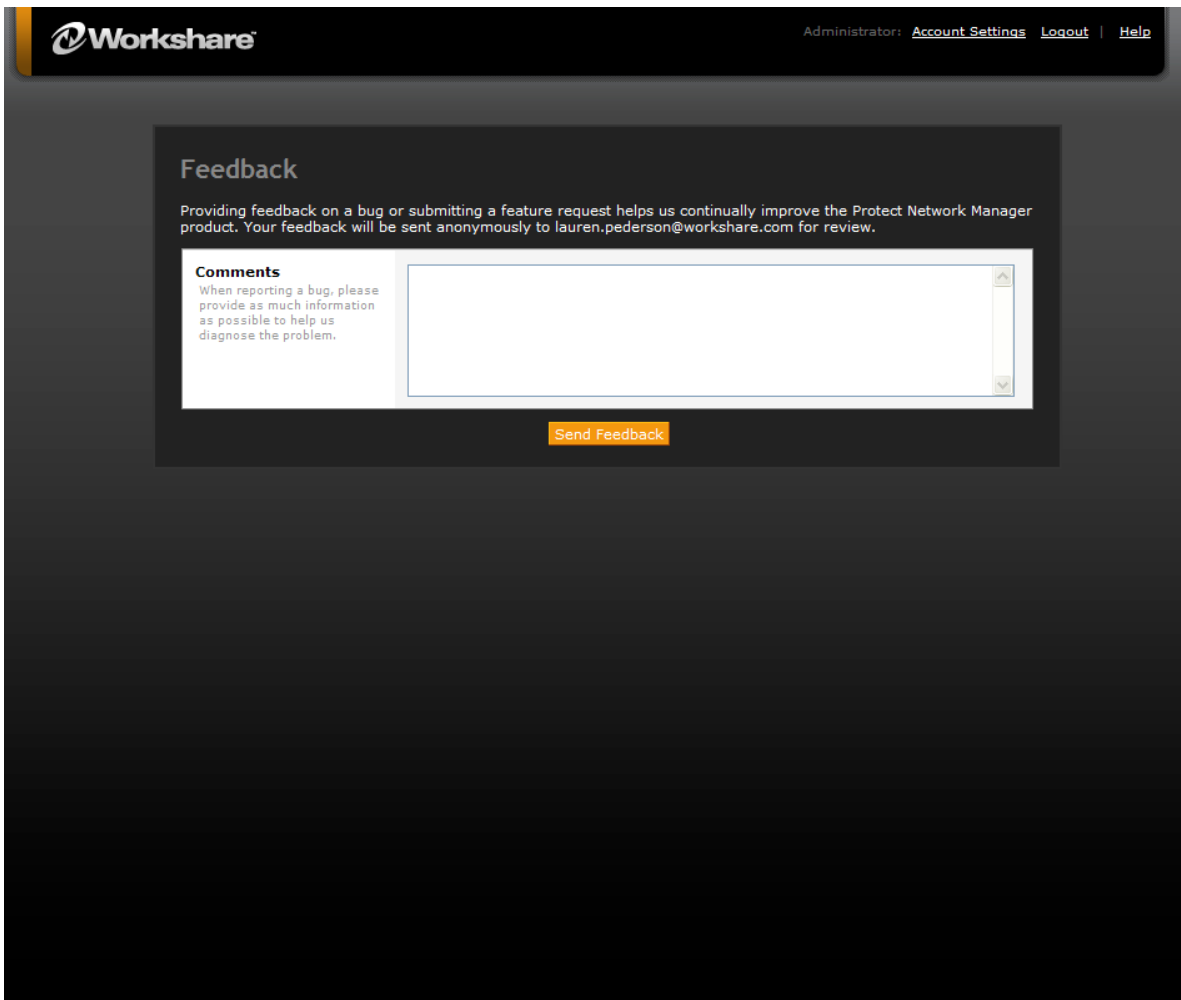


## Sending Feedback

Occasionally you may be prompted to provide feedback on the Workshare Protect Network Manager. When a bug is discovered, the **Feedback** page will automatically display.

To provide feedback, perform the following steps:

1. Type a description of the problem in the **Comments** field, being as descriptive as possible. For example, it is helpful to include details about the actions that were taken just before the **Feedback** page displayed, what the expected behavior was, and any other comments or information that might be relevant to uncovering the source of the problem, or enhancing the Protect Network Manager functionality.



**Workshare** Administrator: [Account Settings](#) [Logout](#) | [Help](#)

### Feedback

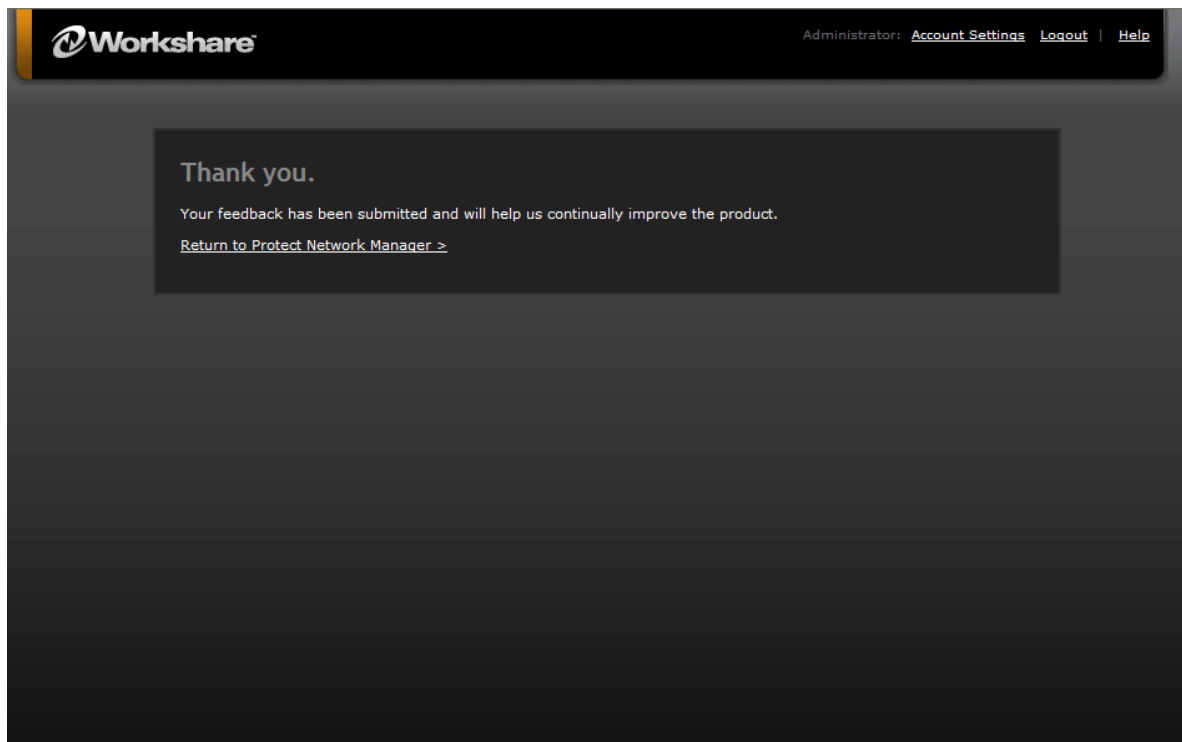
Providing feedback on a bug or submitting a feature request helps us continually improve the Protect Network Manager product. Your feedback will be sent anonymously to [lauren.pederson@workshare.com](mailto:lauren.pederson@workshare.com) for review.

**Comments**  
When reporting a bug, please provide as much information as possible to help us diagnose the problem.

[Send Feedback](#)

2. Click the **Send Feedback** button.

The Thank you page displays to verify that your feedback has been submitted.



3. Click the [Return to Protect Network Manager >](#) to return to the Protect Network Manager.

---

## Chapter 3: Reviewing Emails

If configured by your administrator, you will be alerted by email when an email you send violates your organization's security policy and as a result is quarantined or bounced (the original email is sent back and not sent to the intended recipients). If your administrator has provided you with the option to review incidents in Workshare Protect Network, you will be able to log in to the Workshare Protect Network Manager to view and perform actions on the email message, including send, block, add notes, share, or change ownership.

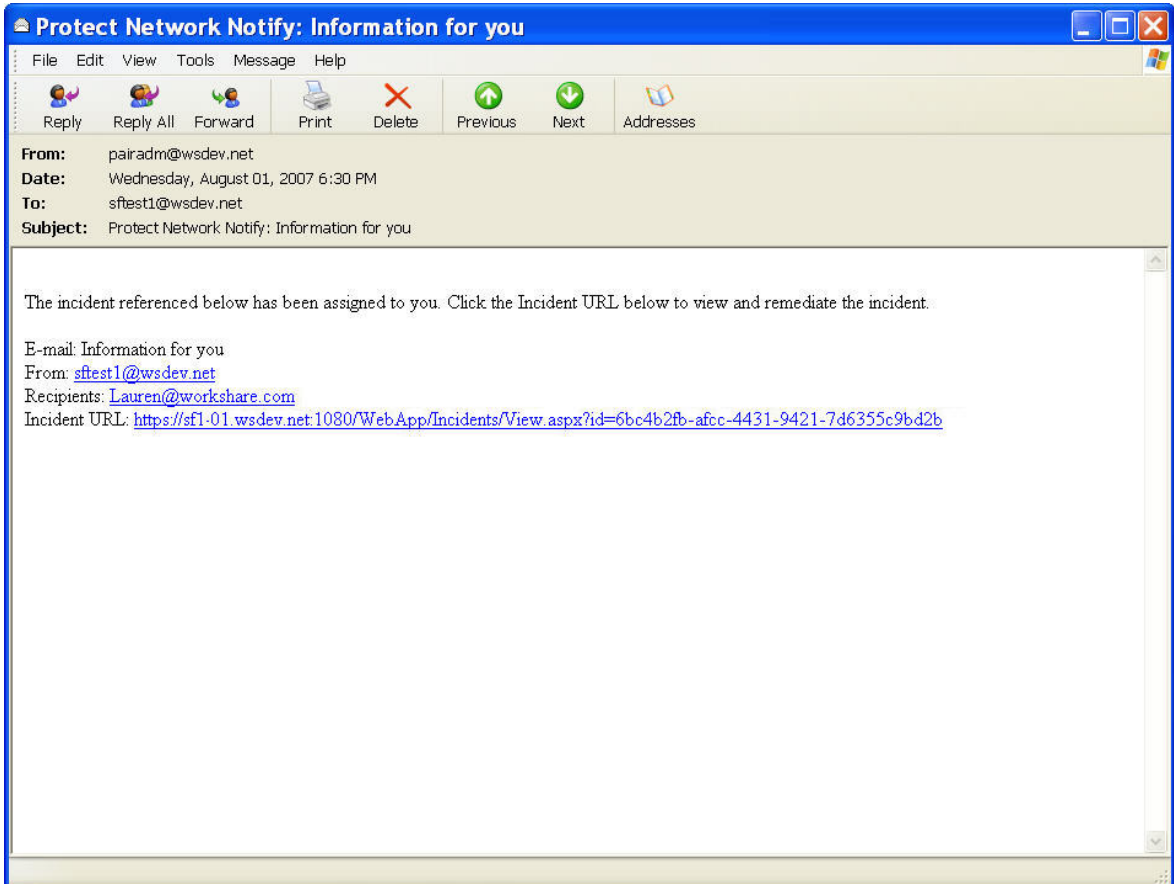
Reviewing Protect Network Notify Emails .....	18
Allowing Emails.....	21
Blocking Emails.....	22
Viewing the Email Contents.....	24
Adding Comments to Email Incidents.....	26
Changing the Email Incident Owner .....	27
Changing the Email Incident Worklist.....	28
Sharing the Email Incident.....	29

## Reviewing Protect Network Notify Emails

When you send an email that violates security policy set by your administrator, you may be notified by a Protect Network Notify email.

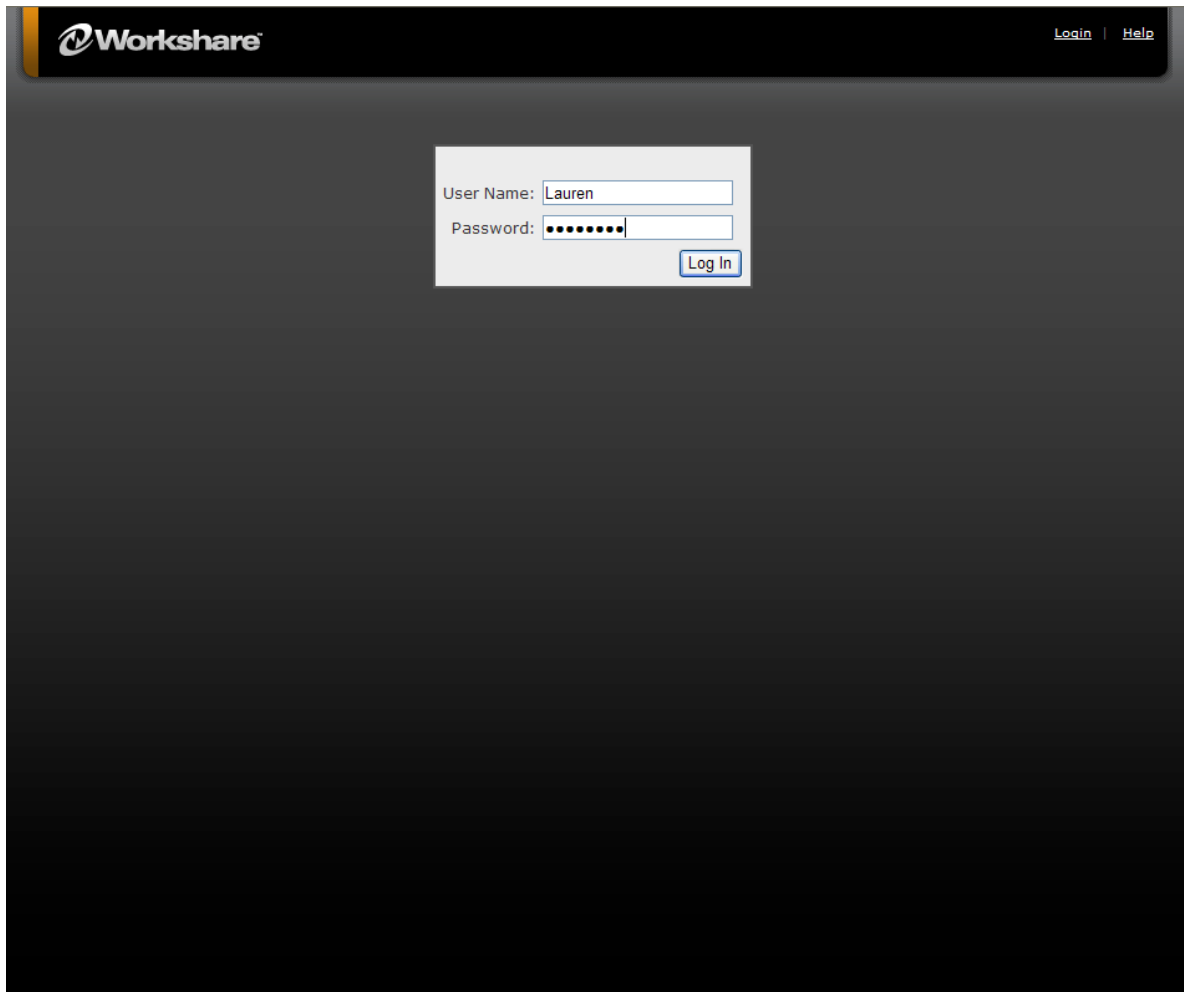
To perform actions on the email, perform the following steps:

1. Click the Incident URL at the bottom of the Protect Network Notify email.



The Workshare Protect Manager log in screen displays.

2. Log in using your username and password, then click **Log in**.



The screenshot shows the Workshare Protect Manager login interface. At the top, there is a dark header with the Workshare logo on the left and "Login | Help" on the right. The main content area is dark gray and features a light gray login form. The form has two input fields: "User Name:" with the text "Lauren" and "Password:" with masked characters (dots). A "Log In" button is positioned to the right of the password field.

The Incidents tab displays with details of the message that violated a security policy.

The screenshot shows the Workshare web interface. At the top, the Workshare logo is on the left, and the user is logged in as Administrator with links for Account Settings, Logout, and Help. Below the navigation bar, there are tabs for Reporting, Incidents (which is active), Fingerprinting, and Management. The main content area shows an incident with the following details:

- Owner: Unassigned
- WorkList: Catch All Worklist
- Buttons: Take Ownership, Change Owner, Change WorkList, Share

On the left side, there is a sidebar with the following options:

- All Open Incidents (highlighted)
- Conflict Worklist
- Catch All Worklist

The incident details include:

- Email: **confidential files** [View Message](#) Allow Block
- From: sftest1@dev.net
- Bcc: belle@gmail.com
- When: 10:09 PM

Below the email details, there is a section for Triggered Policies:

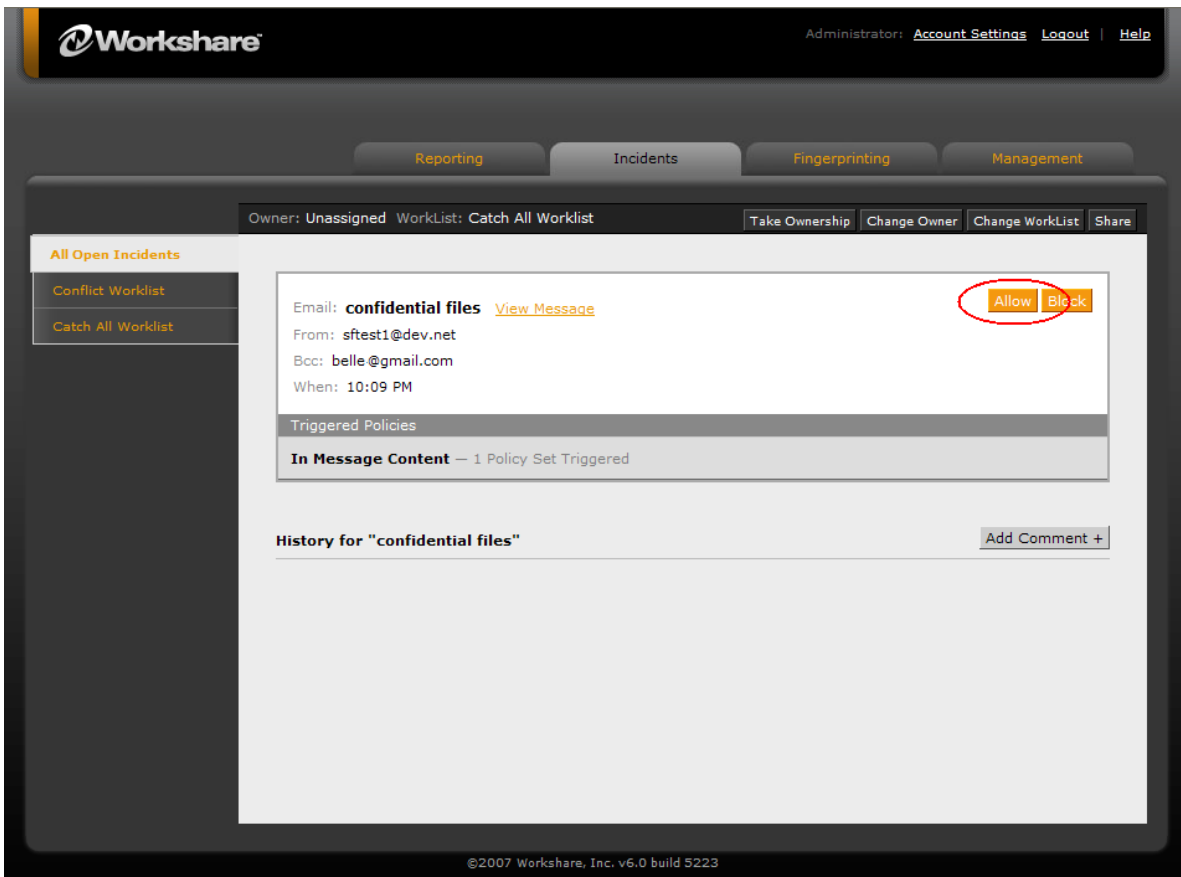
- In Message Content** — 1 Policy Set Triggered

At the bottom of the incident details, there is a section for History for "confidential files" with an [Add Comment +](#) button.

©2007 Workshare, Inc. v6.0 build 5223

## Allowing Emails

1. To allow the message to be sent, click the **Allow** button.



2. Optionally type a comment in the **Comments** field and lick **Allow**. Recipient



3. Check the **Close incident after releasing** to close the incident in the Workshare Protect Network Manager. If this box is not checked, the incident will remain open in the Workshare Protect Network Manager and will need to be manually closed.

## Blocking Emails

1. To block the email from being sent, click the **Block** button.

The screenshot displays the Workshare web application interface. At the top, the Workshare logo is on the left, and the user's role 'Administrator' with links for 'Account Settings', 'Logout', and 'Help' is on the right. Below the header is a navigation bar with tabs for 'Reporting', 'Incidents', 'Fingerprinting', and 'Management'. The main content area shows an incident summary with the following details:

- Owner: Unassigned
- WorkList: Catch All Worklist
- Buttons: Take Ownership, Change Owner, Change WorkList, Share

The incident details include:

- Email: **confidential files** (with a 'View Message' link)
- From: sftest1@dev.net
- Bcc: belle@gmail.com
- When: 10:09 PM

Below the email details is a section for 'Triggered Policies' which shows:

- In Message Content** — 1 Policy Set Triggered

At the bottom of the incident view, there is a 'History for "confidential files"' section with an 'Add Comment +' button. The 'Block' button in the top right corner of the email details is circled in red.

©2007 Workshare, Inc. v6.0 build 5223

2. Check the box next to **Notify Original Sender** to notify the original sender that the email will not be sent.

Block Message CLOSE

**Block Email Delivery**  
 Notify Original Sender

FROM Admin@dev.net  
TO sftest1@dev.net  
CC   
SUBJECT Protect Network Bounce: [#subject#]

Include Original Message

Paragraph Font Name Size **B** *i* U [List Icons]

The email message referenced below contains information that Workshare Protect Network has determined may violate one or more of your organization's security policies and has not been sent. Please review and remediate the content of this email.

E-mail: [#subject#]  
From: [#sender#]  
Recipients: [#recipients#]

Cancel Send  Close Incident After Blocking Email

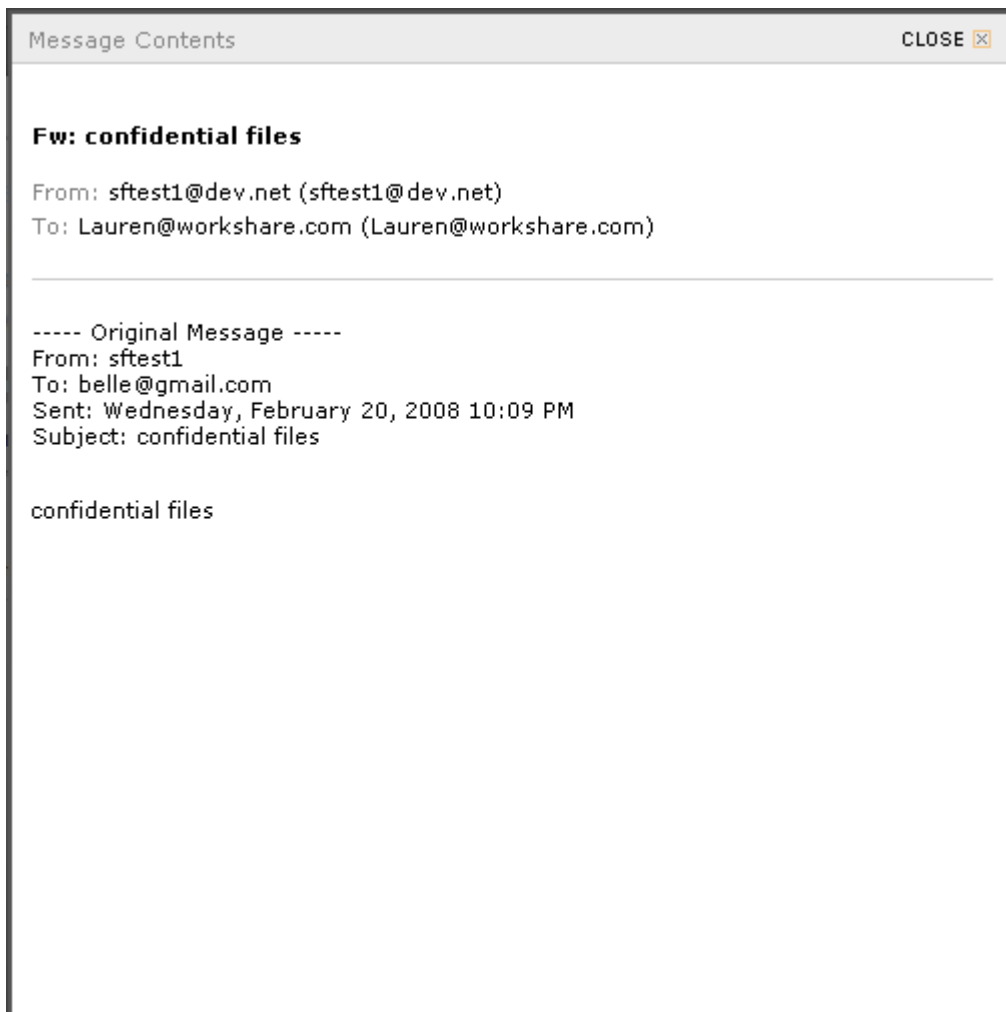
3. Optionally add additional recipients in the CC field.
4. Optionally modify the contents of the notification email.
5. Check the **Close Incident After Blocking Email** to close the incident in the Workshare Protect Network Manager. If this box is not checked, the incident will remain open in the Workshare Protect Network Manager and will need to be manually closed.

## Viewing the Email Contents

1. To view the email contents, click the **View Message** link.

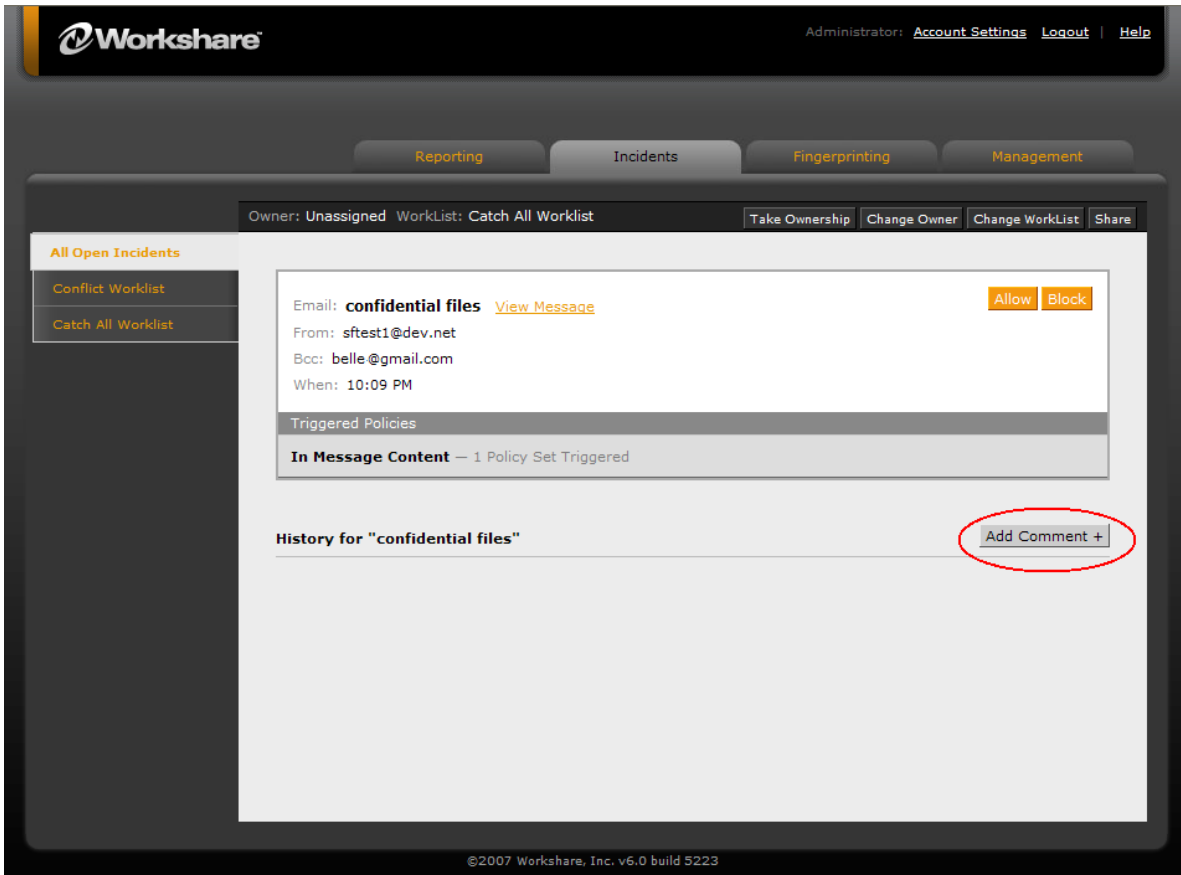
The screenshot displays the Workshare web interface. At the top, the Workshare logo is on the left, and the user's role 'Administrator' with links for 'Account Settings', 'Logout', and 'Help' is on the right. Below the header is a navigation bar with tabs for 'Reporting', 'Incidents', 'Fingerprinting', and 'Management'. The 'Incidents' tab is active, showing a list of incidents. The selected incident is titled 'confidential files' and has a 'View Message' link circled in red. The incident details include the email subject, sender (sftest1@dev.net), recipient (belle@gmail.com), and time (10:09 PM). There are 'Allow' and 'Block' buttons next to the subject. Below the email details is a section for 'Triggered Policies' which shows 'In Message Content' with a note that 1 policy set was triggered. At the bottom of the incident view is a 'History for "confidential files"' section with an 'Add Comment +' button. The footer of the interface reads '©2007 Workshare, Inc. v6.0 build 5223'.

The message displays.

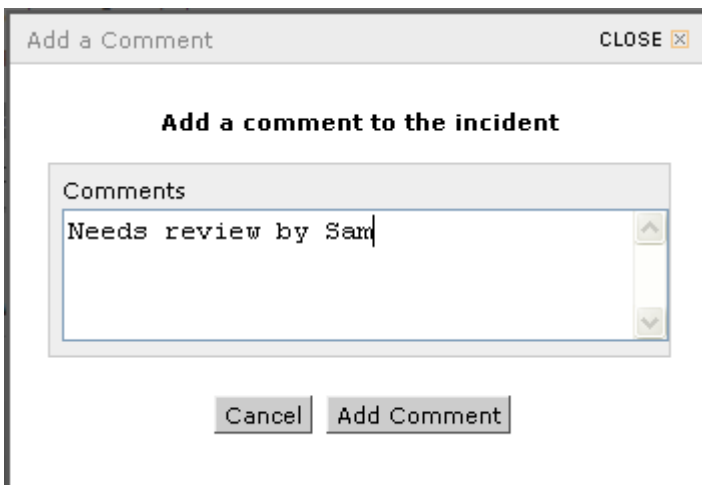


## Adding Comments to Email Incidents

1. To add a comment to the email incident in the Workshare Protect Network Manager, click the **Add Comment** button.

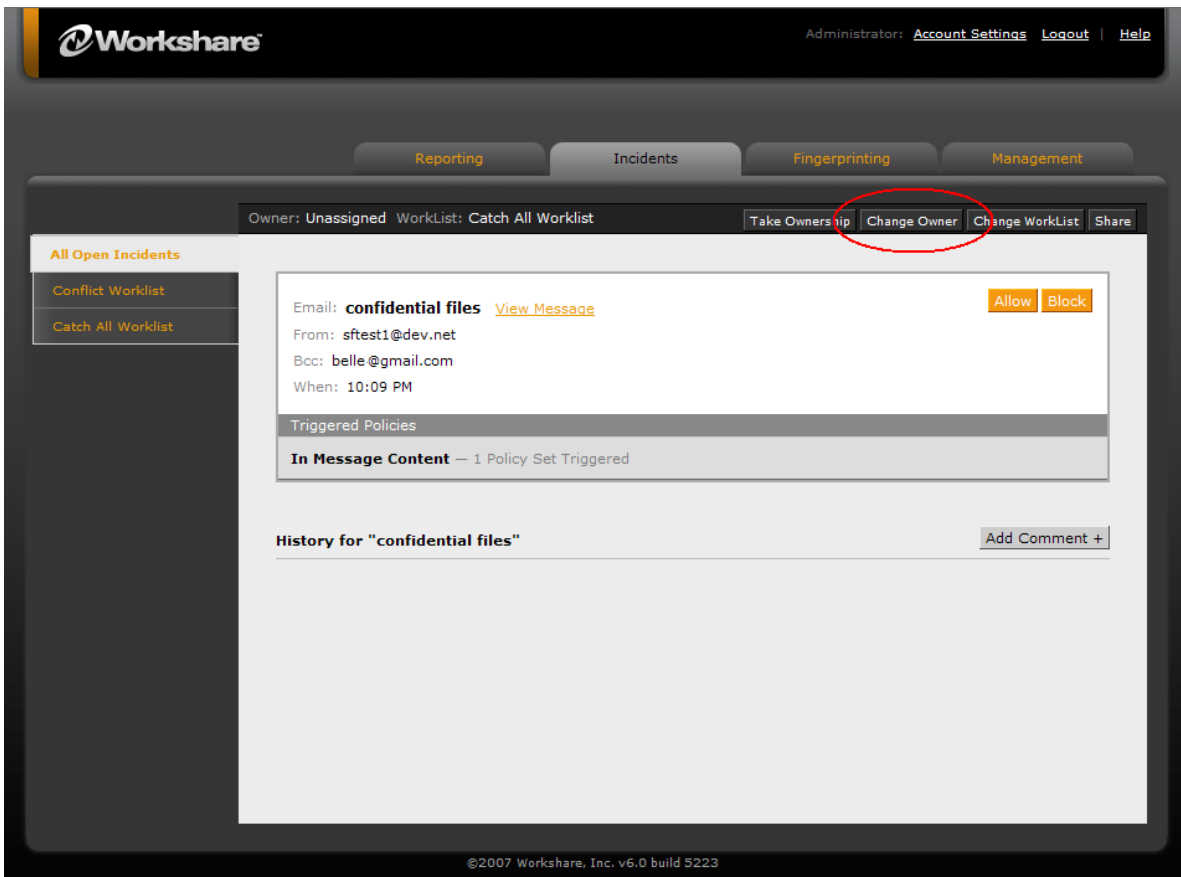


2. Type the comment in the **Comments** field and click **Add Comment**.

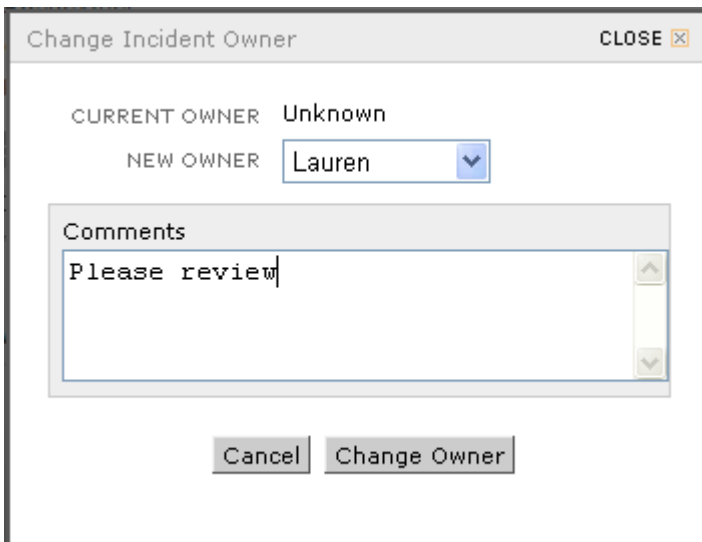


## Changing the Email Incident Owner

1. To change the email incident owner, click the **Change Owner** button.



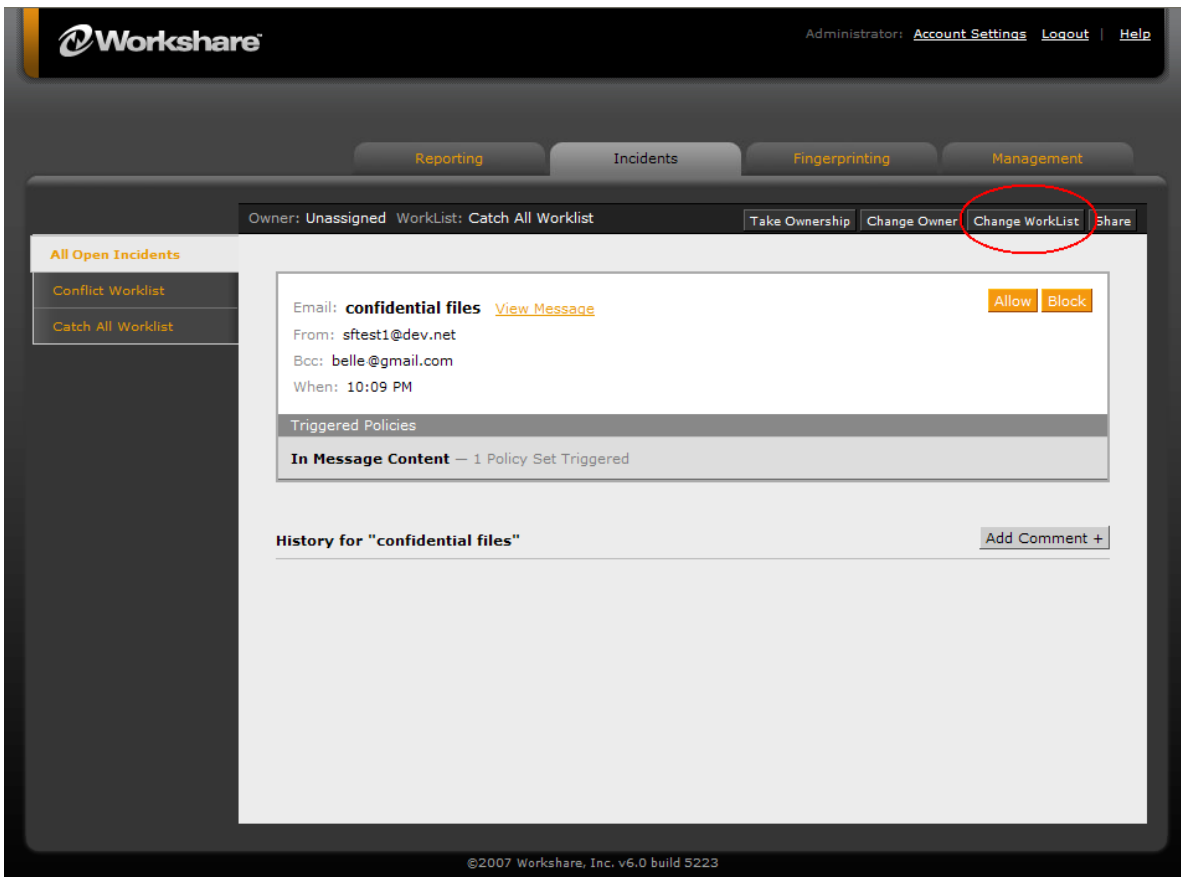
2. Select a new owner from the **New Owner** list and optionally type a comment in the **Comment** field.



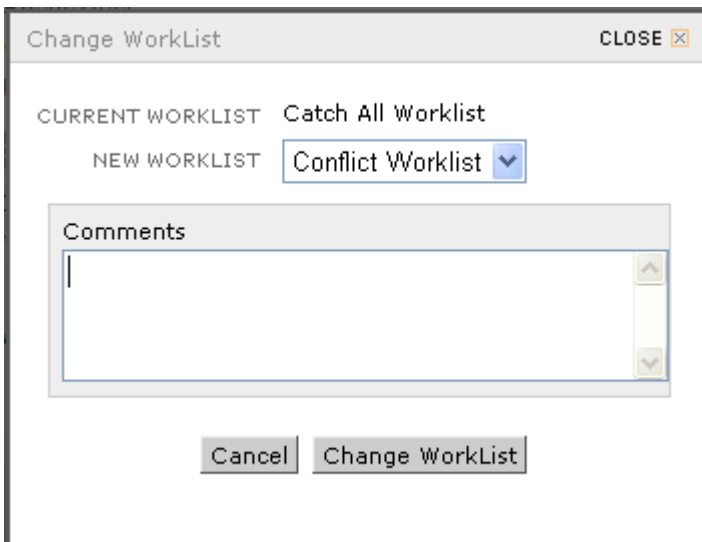
3. Click **Change Owner**.

## Changing the Email Incident Worklist

1. To change the email incident worklist, click the **Change Worklist** button.



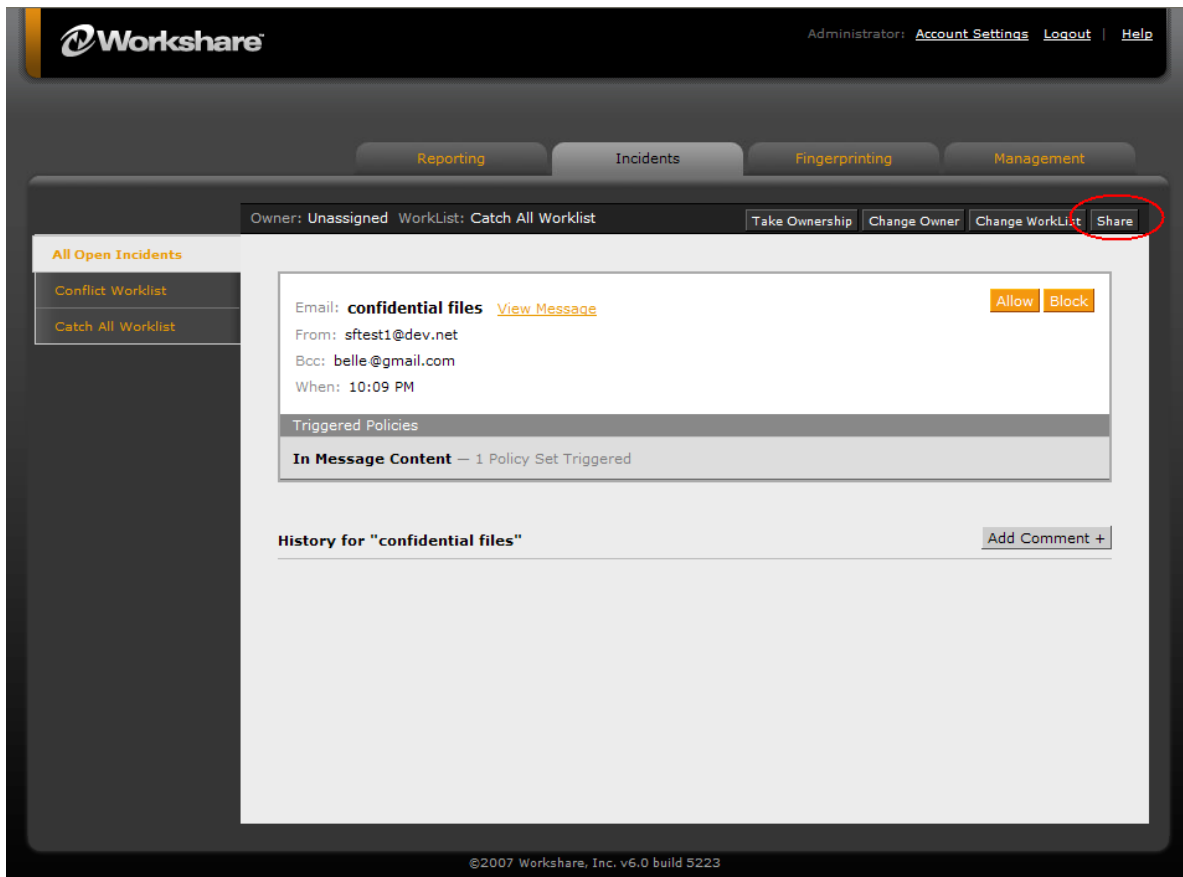
2. Select a new worklist from the **New Worklist** list and optionally add comments in the **Comment** field.



3. Click Change Worklist.

## Sharing the Email Incident

1. To share the email incident, click the **Share** button.



The screenshot displays the Workshare web application interface. At the top, the Workshare logo is on the left, and the user's role 'Administrator' with links for 'Account Settings', 'Logout', and 'Help' is on the right. Below this is a navigation bar with tabs for 'Reporting', 'Incidents', 'Fingerprinting', and 'Management'. The 'Incidents' tab is active, showing a list of incidents. The selected incident is titled 'confidential files' and has a 'Share' button circled in red. The incident details include the email subject 'confidential files', sender 'sftest1@dev.net', recipient 'belle@gmail.com', and time '10:09 PM'. There are 'Allow' and 'Block' buttons next to the subject. Below the email details, a section titled 'Triggered Policies' shows 'In Message Content' with '1 Policy Set Triggered'. At the bottom, there is a 'History for "confidential files"' section with an 'Add Comment +' button. The footer of the page reads '©2007 Workshare, Inc. v6.0 build 5223'.

2. Type the email of the recipient(s) in the **To** and **CC** fields.

Share Incident CLOSE

FROM Admin@local

TO sam@workshare.com

CC

SUBJECT Protect Network Notify: [#subject#]

Include Original Message

The email message referenced below contains information that Workshare Protect Network has determined may violate one or more of your organization's security policies.

E-mail: [#subject#]  
From: [#sender#]  
Recipients: [#recipients#]

Cancel Send

3. Optionally modify the **Subject** field.
4. Check the **Include Original Message** checkbox to include the original message with this message.
5. Optionally modify the contents of the email.
6. Click **Send**.

---

## Appendix E: Customer Support

This appendix provides information about related documentation, the Workshare Knowledge Base, and Workshare customer support services.

### Related Technical Documentation

For detailed information about Workshare Protect Premium, refer to the following technical documentation, available on the Workshare Web site at [www.workshare.com/support/learningcenter](http://www.workshare.com/support/learningcenter):

- Workshare Protect Network Release Notes

### Workshare Knowledge Base

The Workshare Knowledge Base provides solutions to common problems experienced when using Workshare Protect.

To search the Knowledge Base:

1. In a Web browser, navigate to <http://www.workshare.com>.
2. Click the **Support** tab at the top.
3. In the **Resource Center** pane on the left, click **Knowledge Base**.
4. Enter relevant keywords in the **Search for** field, for example, email protection.
5. Select the family of articles to search in the **\*in** dropdown list.
6. Click **Find Article** to display a list of results.
7. Click a link to display the article of your choice.