



## Workshare Protect Network Getting Started Guide

The Workshare Protect Network Getting Started Guide provides instructions for initial setup and configuration of your Workshare Protect Network appliances.

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 Webmail. By deploying Workshare Protect Network, organizations can audit and control outbound traffic at the network gateway.

To obtain the full set of Workshare Protect documents, including advanced deployment guides, administration guides, user guides, and more, visit the Workshare Learning Center on the Workshare Web site, located at:

<http://www.workshare.com/support/learningcenter>

Chapter 1: Before You Begin .....	2
Chapter 2: Choose a Deployment Architecture.....	4
Chapter 3: Installing the Appliance .....	7
Chapter 4: Configuring Workshare Protect Network .....	10
Appendix A: Configuring BlackBerry Enterprise Server (BES).....	13
Appendix B: Configuring an Alternate IP Address.....	15
Appendix C: Appliance Overview.....	16

---

# Chapter 1: Before You Begin

This chapter provides an overview of the Workshare Protect Network, including an introduction to its key components.

This chapter includes the following sections:

- Verify Package Contents
- Installation Prerequisites
- Collect the Following Information

## Verify Package Contents

The following is a list of package contents that should be verified prior to installation:

- One PN-1000 or PN-5000 appliance
- One crossover network cable
- One standard network cable
- One Release Notes document

## Installation Prerequisites

The following prerequisites must be met before the Workshare Protect Network appliance is deployed:

- Network switch that supports SPAN (for example: Cisco, 3Com, Intel) or a network TAP aggregator (for example: NetOptics iTAP Port Aggregator)
- One available Ethernet port
- Appliance administration workstation
- Laptop (if network does not have DHCP)
- Keyboard, monitor and mouse (if network has DHCP)



**Note:** using a laptop for appliance administration, the alternate IP configuration should be pre-configured with the following values: IP address 192.168.11.2, subnet mask 255.255.255.0, and default gateway 192.168.11.1. For instructions on setting up the alternate IP configuration, refer to **Configuring an Alternate IP Address** on page 15.

## Collect the Following Information

Record the following information prior to configuring your Workshare appliance. If you have a DHCP server, this information is not necessary.

IP Address ____.____.____.____	A static IP address for the Workshare appliance that is within the range of the local subnet
Subnet Mask ____.____.____.____	The subnet mask for the local subnet
Default Gateway ____.____.____.____	The IP address of the network's gateway device
Preferred DNS ____.____.____.____	DNS server information
Alternate DNS ____.____.____.____	Optional alternate DNS server information
WINS server (if available) ____.____.____.____	Optional IP address of a WINS server

If configuring a Workshare MTA, record the following additional information:

Mail server _____	The IP address or hostname of the mail server
End point _____	The IP address or hostname of the end point
Authorized address(es) _____	The allowed IP subnet or a single allowed IP address from the mail server or other source(s) of mail traffic.
Mail hostname and port _____	Your company's email server hostname and port

---

## Chapter 2: Choose a Deployment Architecture

This chapter provides information about the architecture and deployment options of the Workshare Protect Network.

This chapter includes the following sections:

- Overview of Architecture
- All in One Deployment
- Distributed Deployment

### Overview of Architecture

When deploying Workshare Protect Network, there are two primary architecture models to choose from, depending on your network topology and size: an All-in-One deployment or a Distributed deployment.

An All-in-One deployment is suitable for organizations with smaller networks, organizations with networks that only have one main connection to the Internet, and organizations that only need to deploy a Workshare MTA or a Workshare Network Monitor.

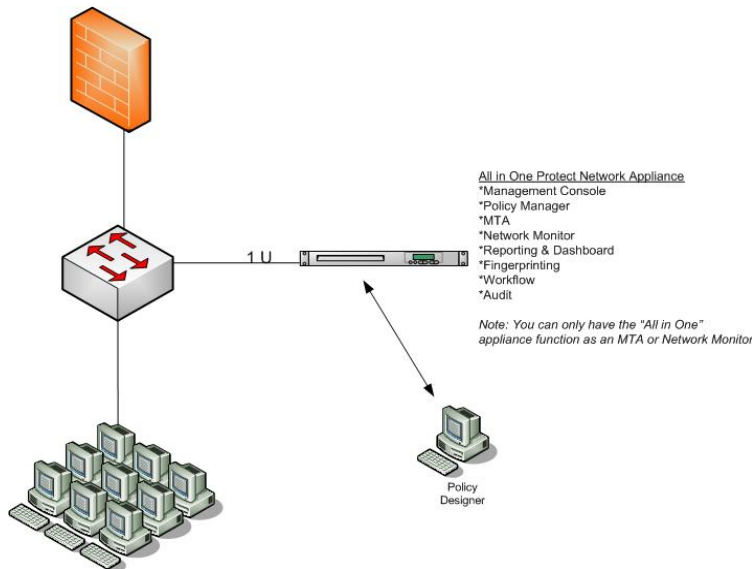
## All-in-One Deployment

The All-in-One deployment has two scenarios: All-in-One: MTA, in which a single appliance is configured as a Workshare MTA, filtering and performing defined actions on network SMTP traffic, or All-in-One: Network Monitor, in which single appliance is configured as a Workshare Network Monitor, monitoring and reporting on network traffic. For information about these deployment scenarios, refer to **All-in-One: MTA** on page 5 or **All-in-One Network Monitor** on page 6.

### All-in-One: MTA

The All-in-One: MTA deployment includes a single appliance that is configured to act as a Workshare MTA. The Workshare MTA inspects outgoing email for policy violations, and if none are found, sends the email to intended recipients. When a policy violation is found, the appropriate action is taken: block, drop, bounce, notify, quarantine, add header, or create incident. The Workshare MTA also provides support for mail sent from Blackberry PDAs, including the ability to block and perform remediation on traffic originating from a PDA. The All-in-One MTA provides the following features and benefits: blocks emails and attachments, blocks emails from BlackBerry devices, user empowerment with self-remediation, fingerprinting for whitelisting and blacklisting, customized workflow, security with customizable user and group permissions, notification when incidents occur. Any SMTP-compliant mail server can be deployed with the All-in-One MTA appliance.

Figure 1: All-in-One: MTA

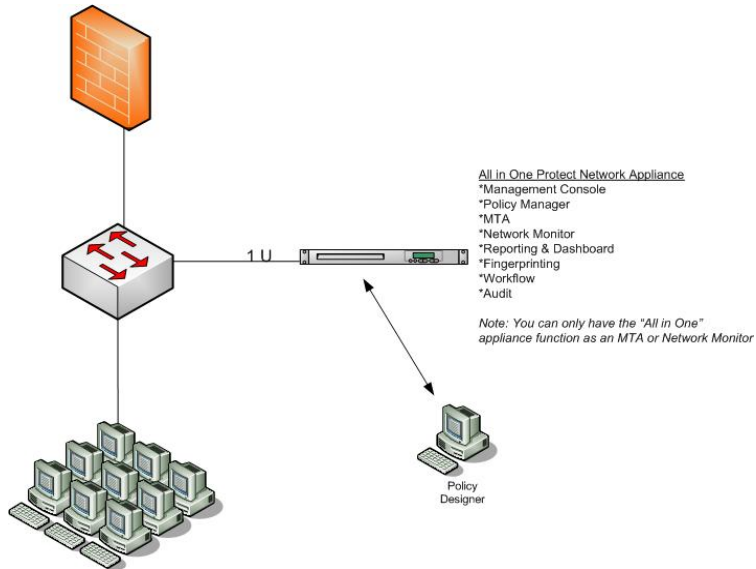


The All-in-One: MTA appliance also includes the Workshare policy manager, management console, reporting, and risk dashboard, fingerprinting service, workflow, and audit service.

## All-in-One: Network Monitor

The All-in-One: Network Monitor deployment includes a single appliance that is configured to act as a 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 and provides alerts and reports. The All-in-One Network Monitor provides the following features and benefits: monitoring of all protocols (HTTP, FTP, SMTP, IM, and Webmail), central reporting, and notifications when incidents occur. Networks must have a network switch that supports port mirroring (SPAN) or a network TAP aggregator device, for example, NetOptics iTAP Port Aggregator.

Figure 2: All-in-One: Network Monitor



The All-in-One: Network Monitor appliance includes the Workshare policy manager, management console, reporting and risk dashboard, fingerprinting, service, workflow, and audit service.

---

## Chapter 3: Installing the Appliance

This chapter provides deployment instructions the Workshare Protect Network.

This chapter includes the following sections:

- Deploying the Appliance
- Connecting the Appliance

### Deploying the Appliance

#### Connecting the Appliance to Your Network

The Workshare appliance(s) will be deployed differently in each network, depending on the choice of deployment (All-in-One: MTA, All-in-One: Network Monitor, or Distributed) and on the other appliances already deployed on the network.

#### Connecting the MTA Appliance

The MTA appliance, when deployed in an All-in-One deployment, is typically installed between a mail server, for example, Exchange Server, and an end point, for example, a mail relay gateway. The MTA must be configured to accept SMTP traffic from the authorized address(es) from or the hostname of the mail server and to forward email to the IP address or hostname of mail relay gateway.

#### Connecting the Network Monitor Appliance

When configured as an All-in-One deployment, the Network Monitor appliance should be positioned as close to the final egress point as possible. However, the Network Monitor appliance should not be deployed between a NAT device or VPN concentrator device and the final egress point.

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



**Note:** Though the Network Monitor appliance analyzes mostly outbound content, it must also have inbound traffic routed through it.

## Logging into the Appliance

This section provides instructions for logging into the Workshare appliance for the first time and setting a static IP address. Refer to the information recorded in the table under **Collect the Following Information on page 3** before logging in and configure an IP address.

To log into the appliance, perform the following steps:

1. Press the power button on the appliance to start it.
2. If the network has a DHCP server, connect the keyboard, monitor and mouse to the appliance. Skip to **step 5**.
3. If the network does not have a DHCP server, plug one end of the crossover cable into the service port of the appliance and the other end into the administration laptop.



**Note:** The alternate IP configuration on the administration laptop should be pre-configured to an IP address of 192.168.11.2, subnet mask of 255.255.255.0, and default gateway of 192.168.11.1.

4. Remote desktop to 192.168.11.1, the default IP address of the Workshare appliance.



**Note:** To access the Remote Desktop Connection, navigate to **Start > All Programs > Accessories > Remote Desktop Connection**.

5. Login using the user name **administrator** and password **workshare**.
6. If you have DHCP, record the IP address of the appliance and the Full Computer Name.
7. If you do not have DHCP, configure a static IP address:
  - Under Network Connections, right-click **Local Area Connection** and select **Properties**.
  - From the **This connection uses the following items** list, select **Internet Protocol (TCP/IP)** and click **Properties**.
  - On the **General** tab, select the radio button next to **Use the following IP address**.
  - In the **IP address** field, type the static IP address for the appliance.
  - In the **Subnet mask** field, type the subnet mask of the network.
  - In the **Default gateway** field, type the IP address of the network gateway.
  - In the Preferred **DNS server** field, type the IP address of the preferred DNS.
  - Optionally configure an alternate DNS by entering the IP of the alternate DNS server in the **Alternate DNS server** field.
  - Record your static IP address and Full Computer Name for remote administration.

## Accessing the Workshare Protect Network Manager

The Workshare Protect Network Manager is a Web-based UI that provides reporting, incident management, and fingerprinting.

To access the Workshare Protect Network Manager, perform the following steps:

1. Launch a Web browser on a workstation connected to the same LAN as the Workshare Protect Network appliance.
2. Type **http://*computername*:1081**, where *computername* is the fully qualified hostname or static IP address of the Workshare Protect Network appliance, in the **Address** or **Location** bar and press Enter.
3. Login using the default username **Administrator** and default password **Workshare1**.



**Note:** For detailed information about using the Workshare Protect Manager, refer to the *Workshare Protect Network Administration Guide*.

## Installing PowerShell

Some features in Workshare Protect Network must be configured using Windows PowerShell.

Windows PowerShell is already installed on the Workshare Protect Network appliance. For instructions on installing Windows PowerShell on a computer for remote administration of the Workshare Protect Network appliance, refer to the *Workshare Protect Network Administration Guide*.

## Installing Workshare Policy Designer

The Workshare Policy Designer is an optional component for the Workshare Protect Network. The Workshare Policy Designer provides additional policy configuration for Workshare Protect MTA and Network Monitor appliances.

For instructions on installing, configuring, and using the Workshare Policy Designer, refer to the *Workshare Protect Deployment Guide* and the *Workshare Policy Administration Guide*.

## Chapter 4: Configuring Workshare Protect Network

This chapter provides configuration instructions the Workshare Protect Network All-in-One: MTA and All-in-One: Network Monitor deployments.

This chapter includes the following sections:

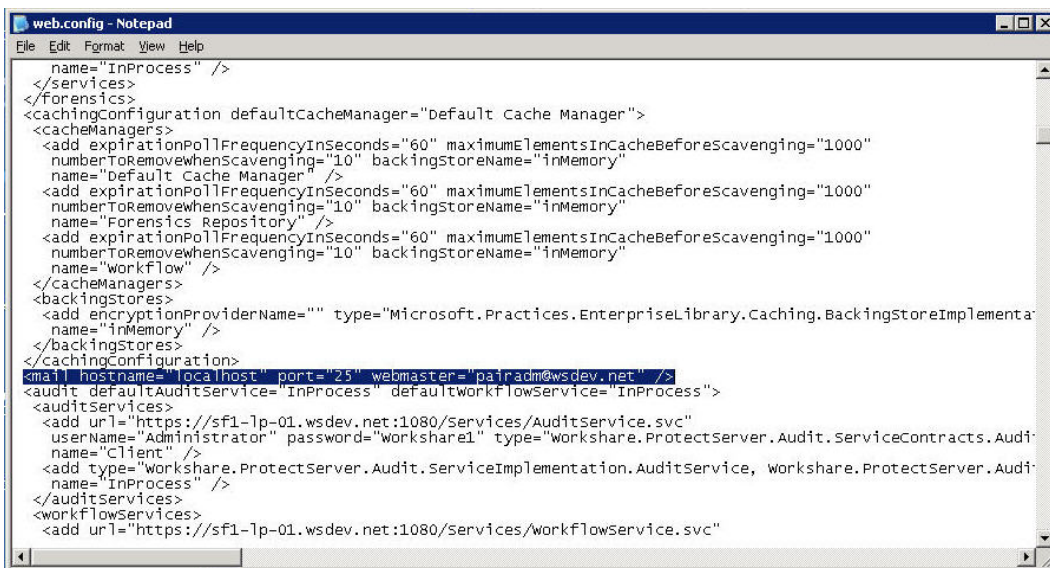
- Configuring the MTA Appliance on page 10
- Configuring the Network Monitor Appliance on page 12

### Configuring the MTA Appliance

Before configuring the appliance as an MTA, refer to the information you recorded in the table under Collect the Following Information on page 3.

To configure the MTA appliance, perform the following steps:

1. On the Workshare Protect Network appliance, navigate to <https://C:\Program Files\Workshare\Protect Server\Web\Tenant\Services\web.config>.
2. In the web.config file, search for the term "mail hostname". Delete "localhost" and type your hostname in quotes. Delete "25" and type your port in quotes. Delete "pairadm@wsdev.net" and type your webmaster email (the email that automatically generated emails will come from) in quotes.



```
web.config - Notepad
File Edit Format View Help
  name="InProgress" />
</services>
</forensics>
<cachingconfiguration defaultCacheManager="Default Cache Manager">
  <cacheManagers>
    <add expirationPollFrequencyInSeconds="60" maximumElementsInCacheBeforeScavenging="1000"
      numberToRemovewhenScavenging="10" backingStoreName="InMemory"
      name="default cache Manager" />
    <add expirationPollFrequencyInSeconds="60" maximumElementsInCacheBeforeScavenging="1000"
      numberToRemovewhenScavenging="10" backingStoreName="InMemory"
      name="Forensics Repository" />
    <add expirationPollFrequencyInSeconds="60" maximumElementsInCacheBeforeScavenging="1000"
      numberToRemovewhenScavenging="10" backingStoreName="InMemory"
      name="workflow" />
  </cacheManagers>
  <backingStores>
    <add encryptionProviderName="" type="Microsoft.Practices.EnterpriseLibrary.Caching.BackingStoreImplementa
      name="InMemory" />
  </backingStores>
</cachingconfiguration>
<mail hostname="localhost" port="25" webmaster="pairadm@wsdev.net" />
<audit defaultAuditService="InProgress" defaultworkflowService="InProgress">
  <auditServices>
    <add url="https://sf1-lp-01.wsdev.net:1080/Services/AuditService.svc"
      userName="Administrator" password="workshare1" type="workshare.ProtectServer.Audit.ServiceContracts.Audi
      name="Client" />
    <add type="workshare.ProtectServer.Audit.ServiceImplementation.AuditService, workshare.ProtectServer.Audi
      name="InProgress" />
  </auditServices>
  <workflowServices>
    <add url="https://sf1-lp-01.wsdev.net:1080/Services/workflowService.svc"
```

3. On the Workshare Protect network appliance, right click **My Computer** and select **Manage**.
4. Expand **Services and Applications** and select **Services**.
5. Right click **Protect Server MTA Services** and select **Properties**.
6. From the **Startup Type** dropdown menu, select **Manual**.
7. Under **Service status**: click the **Start** button.

8. Click OK.
9. On the Workshare Protect Network appliance, launch Windows PowerShell.
10. Type the following command:

```
set-executionpolicy unrestricted
```

11. Type the following command to restart PowerShell:

```
Powershell
```

12. To connect to the MTA service, type the following:

```
Connect-MtaService -username ProtectServerMtaUser -Password  
Workshare1
```

13. Type the following to test your MTA connection:

```
Get-MtaSettings
```

If you see the message "The caller was not authenticated by the service," you have not been successfully connected to the MTA service and should try again, verifying that everything is spelled correctly.

```
PS C:\Documents and Settings\Administrator> Get-MtaSettings  
Get-MtaSettings : The caller was not authenticated by the service.  
At line:1 char:15  
+ Get-MtaSettings <<<<
```

If you see a list of MTA settings, you have successfully connected to the MTA service.

```
PS C:\Documents and Settings\Administrator> Get-MtaSettings  
  
ProcessMail           : True  
MailGateway           :  
ConnectionTimeout     : 200000  
AuthorizedAddresses   : {10.0.4.0/24}  
IdleTimeout           : 200000  
MaxConnections        : 100  
MinThreads            : 25  
MaxThreads            : 120
```

14. To update the mail gateway, type the following, where *x.x.x.x* is the IP address of the end point:

```
Update-MtaSettings -MailGateway x.x.x.x
```

15. To update the MTA authorized address(es), type the following, where *x.x.x.x/xx* is an allowed IP subnet and *x.x.x.x* is a single allowed IP address from the mail server or other source(s) of SMTP traffic:

```
Update-MtaSettings -AuthorizedAddresses x.x.x.x/xx, x.x.x.x
```

16. To apply the changes, type the following, where the parameter *1* means true:

```
Update-MtaSettings -ApplyNow 1
```

17. Optionally type the following cmdlet to view and verify your changes:

```
Get-MtaSettings
```

18. Before exiting Windows PowerShell, type the following command:

```
set-executionpolicy restricted
```

19. Exit PowerShell.

For instructions for configuring a BlackBerry Enterprise Server (BES), refer to Configuring a BlackBerry Enterprise Server on page 12.

**Tip:** For advanced configuration instructions, refer to the *Workshare Protect Network Administration Guide*



To remotely administer the MTA service after initial configuration, launch PowerShell on a remote administration computer, and type the following command, where *computername* is the fully qualified computer name or IP address of the Workshare Protect Network appliance, *Sam* is the username and *password123* is the user password:

```
Connect-MtaService -hostname computername -UserName Sam -Password  
password123
```

## Configuring the Network Monitor Appliance

To configure Network Monitor appliance, perform the following steps:

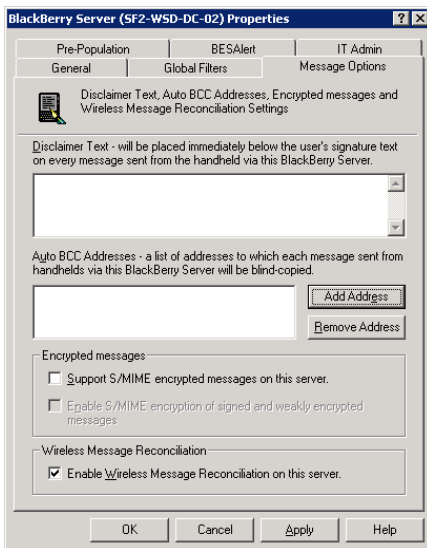
1. Launch Windows PowerShell on the Workshare Protect Network appliance.
2. Type the following command:  
`set-executionpolicy unrestricted`
3. Type the following command to restart PowerShell:  
`Powershell`
4. Type the following to enable the Network Monitor:  
`Set-NetMonitorSettings -enabled 1`
5. Type the following to start the Network Monitor service:  
`Start-Service "Protect Server Network Monitor Service"`
6. Type the following start the Protocol Analysis service:  
`Start-Service "Protect Server Protocol Analysis Service"`
7. Before exiting Windows PowerShell, type the following command:  
`set-executionpolicy restricted.`
8. Exit PowerShell.

---

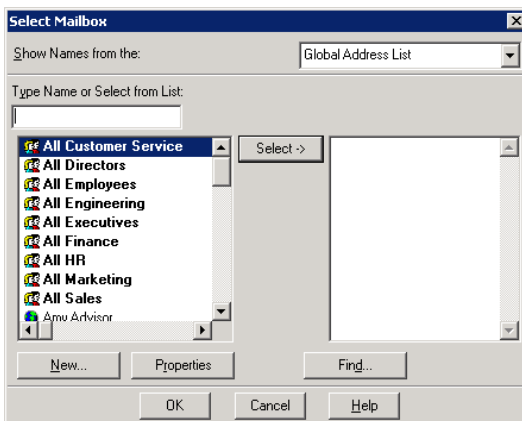
# Appendix A: Configuring BlackBerry Enterprise Server (BES)

To configure the BlackBerry Enterprise Server (BES) to work with the Workshare MTA appliance, perform the following steps:

1. Launch the BlackBerry Manager.
2. Click **Blackberry Server Properties**.
3. Select the **Message Options** tab and click **Add Address**.

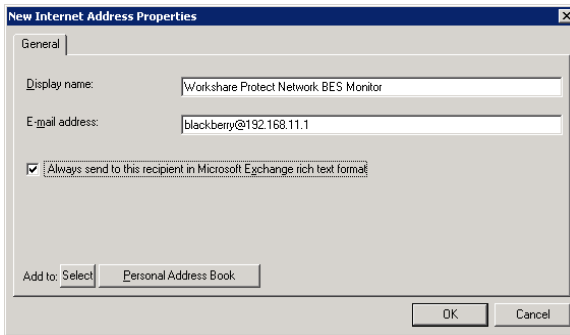


4. Click **New**.

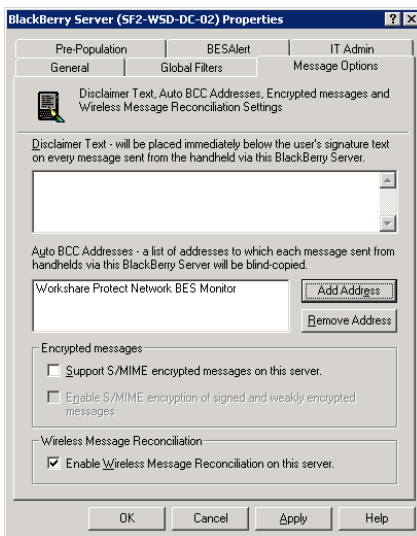


5. Select the **Internet Address** and select the radio button next to **In this message only**. Click **OK**.
6. Type an identifying display name in **Display name**.

7. Type blackberry@192.168.11.1 in the E-mail address field. Click OK.



8. When the BlackBerry address has been configured successfully, it will display on the Message Options tab.



---

## Appendix B: Configuring an Alternate IP Address

When installing a Workshare Protect Network appliance on a network without DHCP, the administration laptop must have an alternate IP configuration.

To configure the alternate IP address for installing an appliance on a network without DHCP, perform the following steps:

1. Under Network Connections, right-click Local Area Connection and select Properties.
2. From the This connection uses the following items list, select Internet Protocol (TCP/IP) and click Properties.
3. Click the Alternate Configuration tab.
4. Select the radio button next to **Use the following IP address**.
5. In the **IP address** field, type 192.168.11.2.
6. In the **Subnet mask** field, type 255.255.255.0.
7. In the **Default gateway** field, type 192.168.11.1.
8. Click **OK**.

---

## Appendix C: Appliance Overview

### Workshare Appliance Hardware Specifications

This section provides the hardware specifications for the Workshare PN-5000 appliance.

#### Workshare PN-1000 Appliance

##### Hardware

- 1 U Appliance
- PENTIUM D 945 3.4GHz
- 4GB of RAM
- 250GB HDD

##### Software:

- Windows 2003 Embedded Server R2
- SQL Server Embedded 2005
- Windows PowerShell
- .NET 2.0



**Note:** In order to perform maintenance tasks on the SQL database, including backing up, restoring, and running scripts to optimize database performance or install patches, it is necessary to access the Workshare Protect Network appliance using remote desktop perform these tasks using the local SQL tools installed on the appliance.

## 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.

## Trademarks

Trademarked names appear throughout this guide as well as 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.