Xerox Multifunction Devices

Customer Tips

… for the user

dc06cc0374
February 20, 2006

WC/WCP 200 Series Audit Log Feature

Purpose

The device audit log is a new feature beneficial to anyone with a requirement to track activities that occur on each device. The information in an audit log is protected by SSL encryption to meet security requirements. This document describes how to configure and generate the Audit Log available on the WC/WCP 232/238/245/255/265/275 devices and the information the log contains.

This document applies to these Xerox products:

x	**WC Pro 232/238/245/255/265/275**
x	**WC 232/238/245/255/265/275**
	WC Pro C2128/C2636/C3545
	WC Pro 165/175
	WC M165/M175
	WC Pro 32/40 Color
	WC Pro 65/75/90
	WC Pro 35/45/55
	WC M35/M45/M55
	DC 555/545/535
	DC 490/480/470/460
	DC 440/432/425/420
	DC 332/340
	DC 265/255/240
	DC 220/230
	DCCS 50

Audit Log Characteristics

The following items impact your use of the audit log:

- The maximum audit log size is 15,000 entries.
- When the maximum is reached, the log begins to overwrite entries.
- The system administrator user ID and password are required to enable, disable, and generate the audit log.

Configuring the Audit Log

Configuration of the audit log requires that tasks are performed in the following order:

- Create or upload and SSL certificate
- Enable SSL
- Enable the audit log

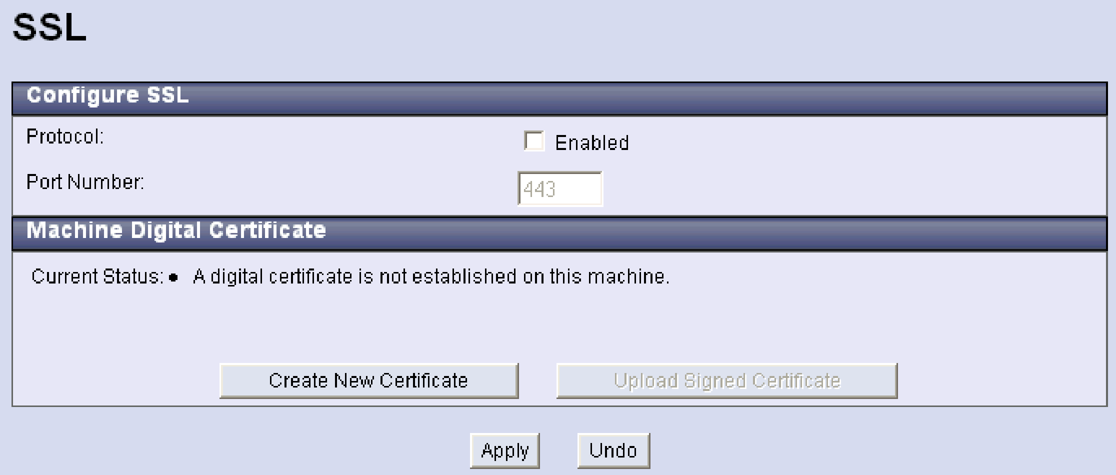
Acquiring an SSL Certificate

The following types of SSL certificates are available:

- **Self Signed Certificate: Establish a Self Signed Certificate on this machine.** This option creates a certificate that is not validated by a Certificate Authority. This type of certificate is used primarily to obtain a key. The information you enter is similar to that required to request an external certificate but it serves no real purpose. A self-signed certificate can expire and still have a valid, usable key. If you enable SSL only to enable the audit log, this selection is probably adequate.
- **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority.** The information on this page is saved in a .pem.txt file that is sent to an external authority who can issue a certificate.

Create a Self Signed Certificate

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **SSL**.



SSL

Configure SSL

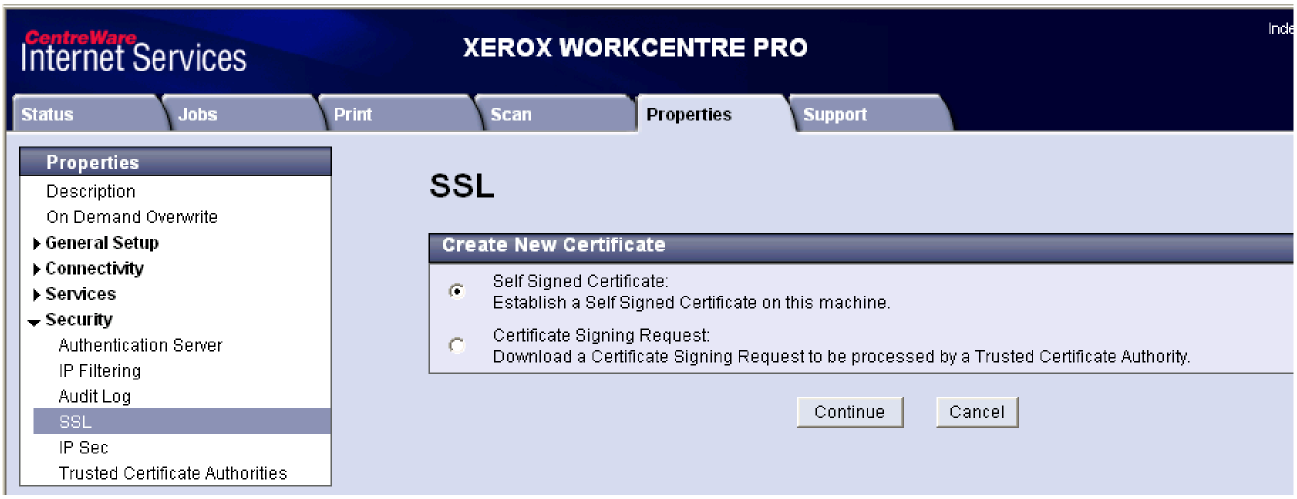
Protocol: □ Enabled

Port Number: 443

Machine Digital Certificate

Current Status: ● A digital certificate is not established on this machine.

2. Click **Create New Certificate**.



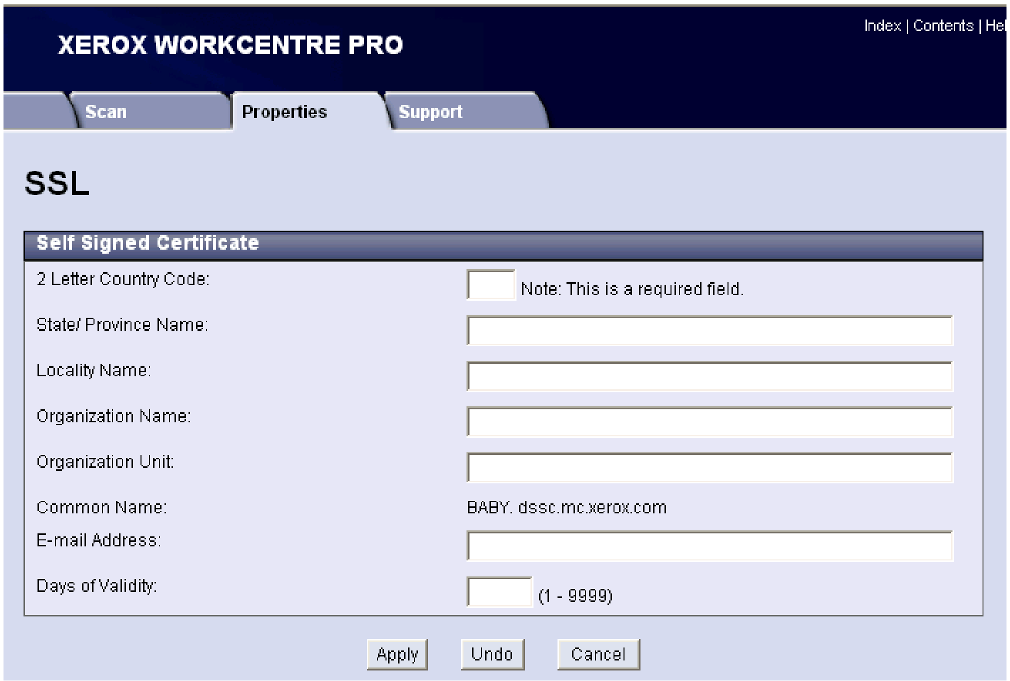
SSL

Create New Certificate

● Self Signed Certificate:
Establish a Self Signed Certificate on this machine.

○ Certificate Signing Request:
Download a Certificate Signing Request to be processed by a Trusted Certificate Authority.

3. Select **Self Signed Certificate: Establish a Self Signed Certificate on this machine** then click **Continue**.



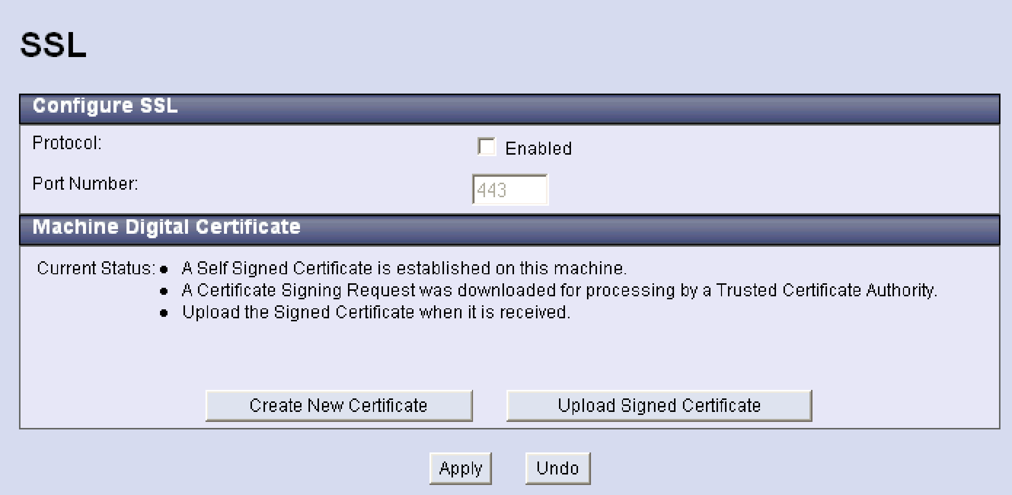
SSL

Self Signed Certificate

2 Letter Country Code:	Note: This is a required field.
State/ Province Name:	
Locality Name:	
Organization Name:	
Organization Unit:	
Common Name:	BABY. dssc.mc.xerox.com
E-mail Address:	
Days of Validity:	(1 - 9999)

Enter information for a self-signed certificate. The country code field entry is required.

4. Click **Apply**. The Administrator Authentication screen may appear. Enter the current User Name and Password and click **OK**. The SSL page appears and shows that the device has a Self Signed Certificate.



SSL

Configure SSL

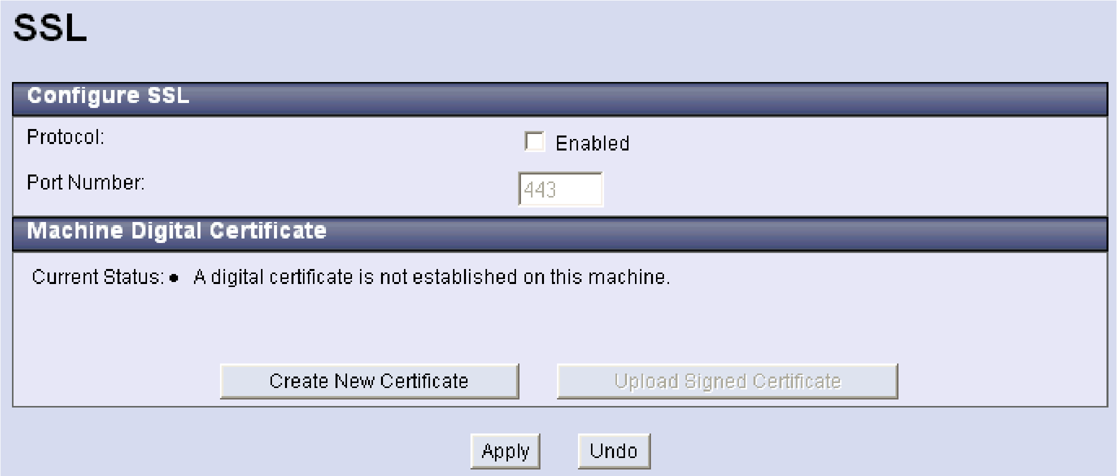
Protocol:	□ Enabled
Port Number:	443

Machine Digital Certificate

Current Status:
- A Self Signed Certificate is established on this machine.
- A Certificate Signing Request was downloaded for processing by a Trusted Certificate Authority.
- Upload the Signed Certificate when it is received.

Create a Certificate Signing Request

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **SSL**.



SSL

Configure SSL

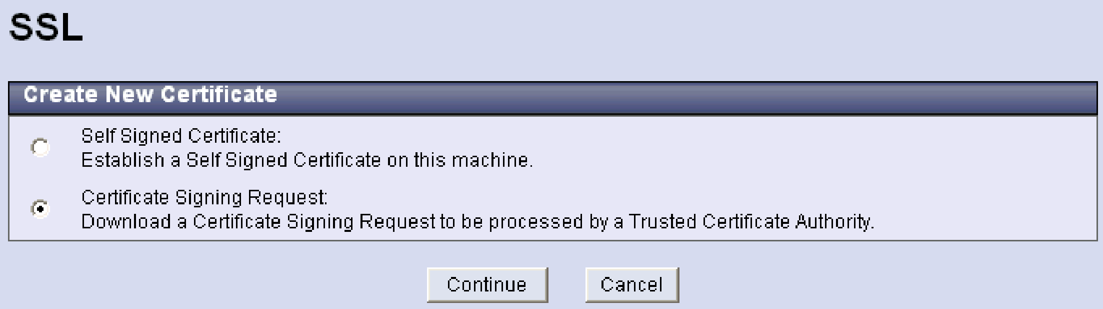
Protocol: □ Enabled

Port Number: 443

Machine Digital Certificate

Current Status: ● A digital certificate is not established on this machine.

2. Click **Create New Certificate**. Select **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** then click **Continue**.



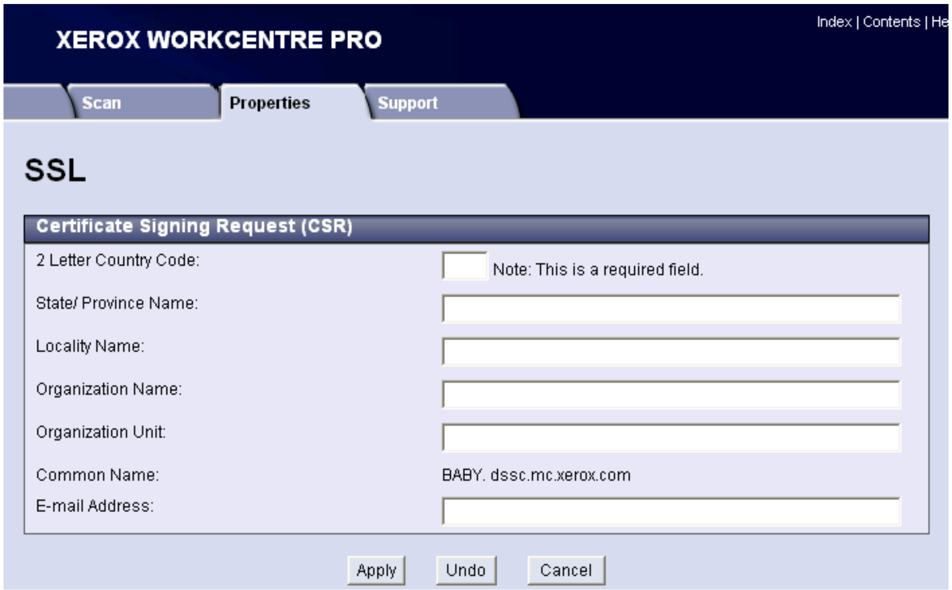
SSL

Create New Certificate

○ Self Signed Certificate:
Establish a Self Signed Certificate on this machine.

● Certificate Signing Request:
Download a Certificate Signing Request to be processed by a Trusted Certificate Authority.

3. Enter the information you wish to appear in your Certificate Signing Request.



SSL

Certificate Signing Request (CSR)

2 Letter Country Code: Note: This is a required field.

State/ Province Name:

Locality Name:

Organization Name:

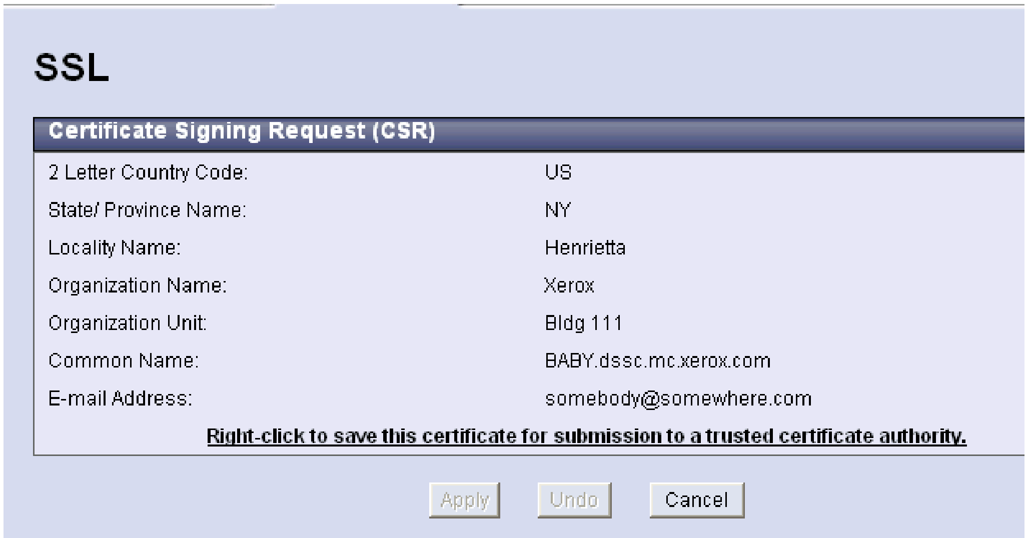
Organization Unit:

Common Name: BABY. dssc.mc.xerox.com

E-mail Address:

4. Click **Apply**. The Administrator Authentication screen may appear. Enter the current User Name and Password and click **OK**.

5. The certificate request information you entered is displayed. Below this data, right-click the link and select **Save Target As**.



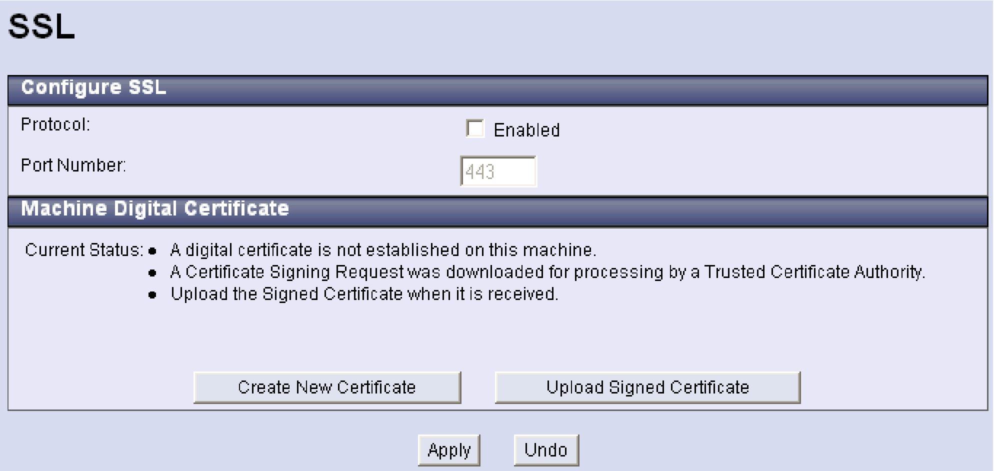
SSL

Certificate Signing Request (CSR)

2 Letter Country Code:	US
State/ Province Name:	NY
Locality Name:	Henrietta
Organization Name:	Xerox
Organization Unit:	Bldg 111
Common Name:	BABY.dssc.mc.xerox.com
E-mail Address:	somebody@somewhere.com

Right-click to save this certificate for submission to a trusted certificate authority.

6. Save the .pem.txt file and send it to a trusted certificate authority. A status message appears on the SSL page indicating a Certificate Signing Request is pending.



SSL

Configure SSL

Protocol: □ Enabled

Port Number: 443

Machine Digital Certificate

Current Status:
- A digital certificate is not established on this machine.
- A Certificate Signing Request was downloaded for processing by a Trusted Certificate Authority.
- Upload the Signed Certificate when it is received.

Uploading the Signed Certificate

You receive notification of the signed certificate in a manner that complies with the policy of the authority issuing the certificate (for example, via email).

1. When you receive the signed certificate, access the SSL page again and click **Upload Signed Certificate**.
2. Click **Browse**, locate the certificate (.pem file), and click **Upload Certificate**.
3. **Current Status** on the SSL page shows a Signed Certificate resides on the device.

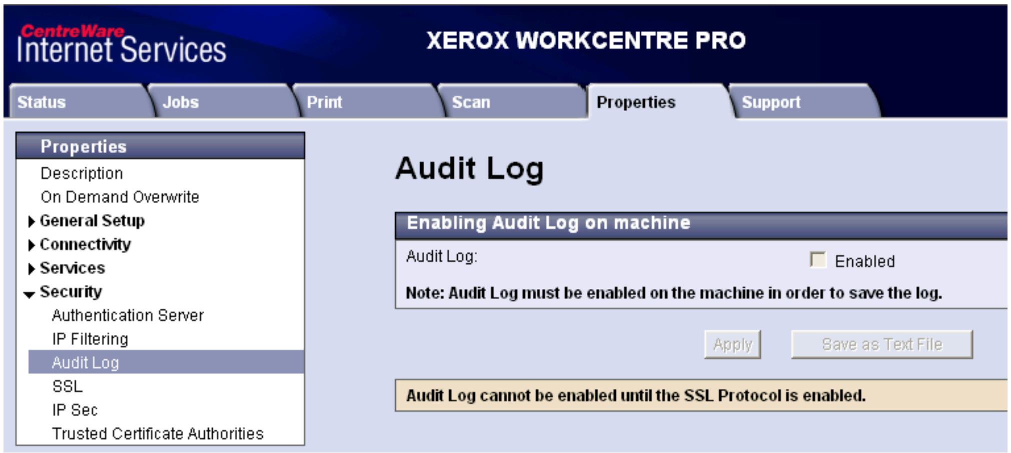
Enable SSL

After a certificate exists you can enable SSL.

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **SSL**.
2. Select the **Protocol Enabled** box and click **Apply**.

Enable the Audit Log

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **Audit Log**.



Audit Log

Enabling Audit Log on machine

Audit Log: □ Enabled

Note: Audit Log must be enabled on the machine in order to save the log.

Audit Log cannot be enabled until the SSL Protocol is enabled.

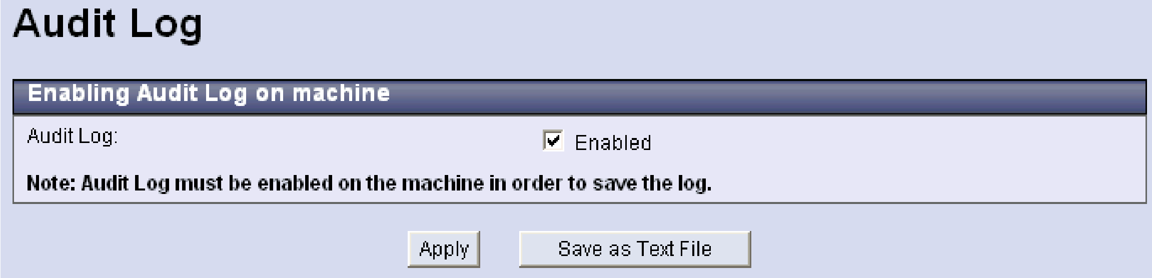
2. The Administrator Authentication screen may appear. Enter the current **User name** and **Password** and click **OK**.

3. Select the **Protocol Enabled** box and click **Apply**.

Generating the Audit Log

To view the Audit Log

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **Audit Log**.



Audit Log

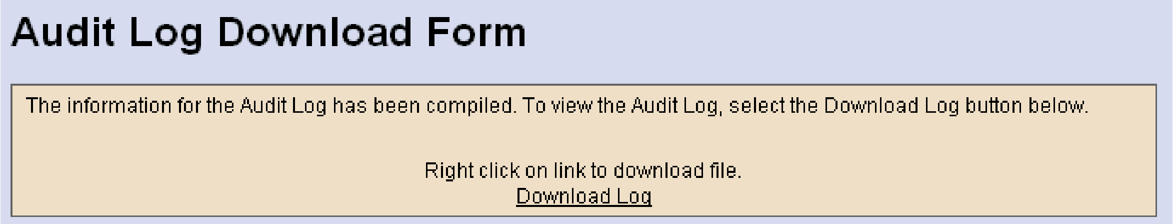
Enabling Audit Log on machine

Audit Log: ☑ Enabled

Note: Audit Log must be enabled on the machine in order to save the log.

2. Click **Save as Text File**. The Administrator Authentication screen may appear. Enter the current **User name** and **Password** and click **OK**.

3. When the Audit Log is ready a page with the following message appears. Right click on **Download Log** and select **Save Target As**.



Audit Log Download Form

The information for the Audit Log has been compiled. To view the Audit Log, select the Download Log button below.

Right click on link to download file.
Download Log

4. Save the file auditfile.gz. It is a zipped file that contains a .txt file. Extract the .txt file.

5. Open Excel and select **File>Open**. Locate the .txt file and click on it. Use the Text Import Wizard to transfer the audit log into Excel.

Audit Log Information

The audit log contains information about most events that occur on a device. Copy and embedded fax jobs are not included in the current version of the audit log feature. All entries contain some common information:

- Entry number
- Date activity occurred
- Time activity occurred
- Event ID
- Event description
- Job name
- User name

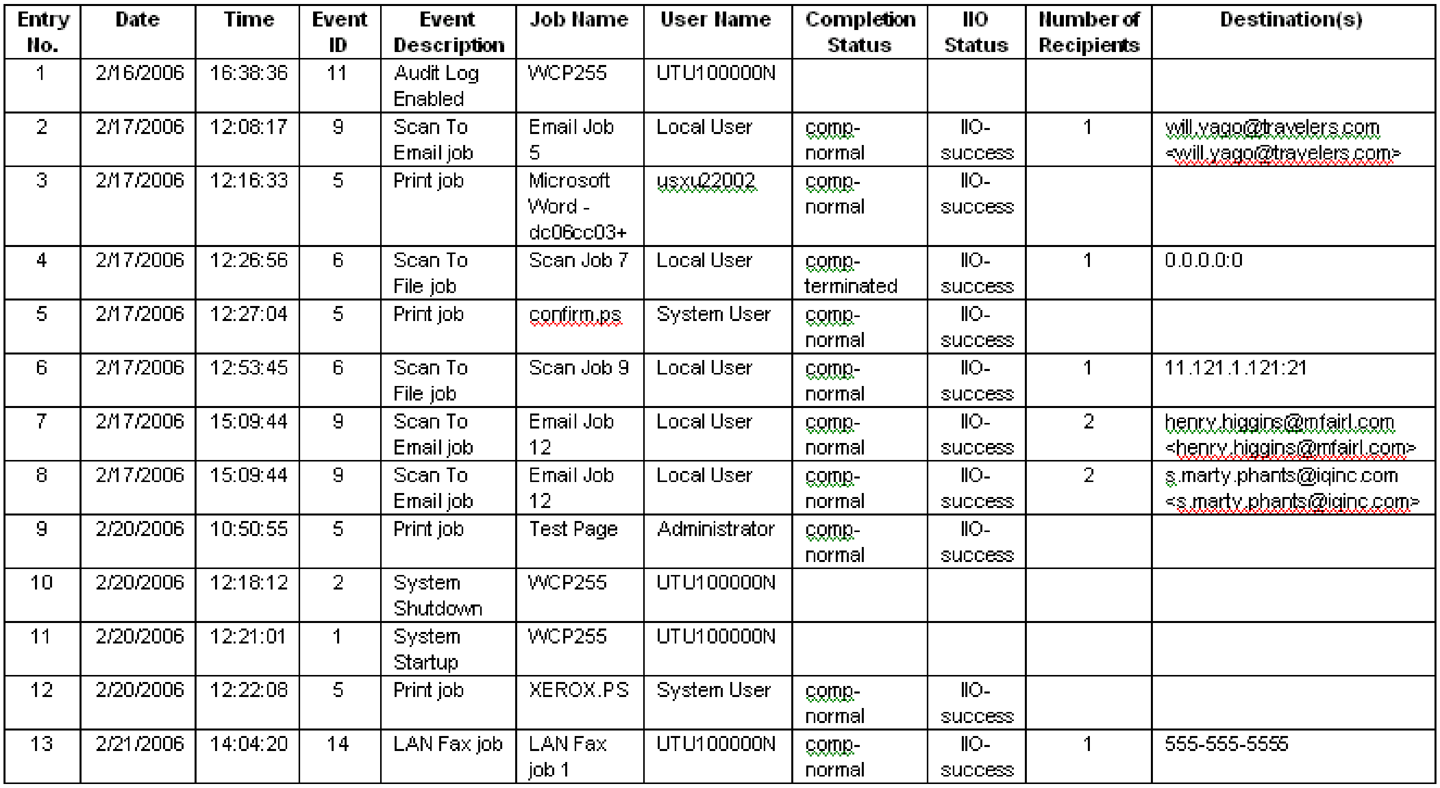
Depending on the event type, other information is also included. The following table lists unique event information that may appear in the audit log.

Event	Information Included in Audit Lob
System startup, system shutdown, ODIO started. ODIO complete, audit log disabled, audit log enabled,	Device name, device serial number
Print job, network scan job, server fax job, Internet fax job, email job, LAN fax job	Completion status, IIO status*, accounting user ID*, accounting account ID*
Server fax job, LAN fax job	Total number of fax phone numbers, fax recipient(s)
Network scan job	Total number of network destinations, network destination
Internet fax job, email job	Total number of SMTP recipients, SMTP destination(s)**

*If enabled.

The following illustrates a sample Audit Log. These points apply to the way log entries appear:

- Audit log fields allow a fixed number of characters. If the number of characters is exceeded, a + sign indicates the data is truncated.
- Scan to file, email, and Internet fax jobs generate multiple audit log entries, one for each job recipient.
- If a LAN fax or server fax job is sent to more than one number, a single audit log entry appears in the audit log that lists the number of recipients. The phone numbers are listed in a single field unless truncated by the character limit.



Entry No.	Date	Time	Event ID	Event Description	Job Name	User Name	Completion Status	I/O Status	Number of Recipients	Destination(s)
1	2/16/2006	16:38:36	11	Audit Log Enabled	WCP255	UTU100000N				
2	2/17/2006	12:08:17	9	Scan To Email job	Email Job 5	Local User	comp-normal	I/O-success	1	will.yago@travelers.com <will.yago@travelers.com>
3	2/17/2006	12:16:33	5	Print job	Microsoft Word - dc06cc03+	usxu22002	comp-normal	I/O-success		
4	2/17/2006	12:26:56	6	Scan To File job	Scan Job 7	Local User	comp-terminated	I/O-success	1	0.0.0.0:0
5	2/17/2006	12:27:04	5	Print job	confirm.ps	System User	comp-normal	I/O-success		
6	2/17/2006	12:53:45	6	Scan To File job	Scan Job 9	Local User	comp-normal	I/O-success	1	11.121.1.121:21
7	2/17/2006	15:09:44	9	Scan To Email job	Email Job 12	Local User	comp-normal	I/O-success	2	henry.higgins@mfairl.com <henry.higgins@mfairl.com>
8	2/17/2006	15:09:44	9	Scan To Email job	Email Job 12	Local User	comp-normal	I/O-success	2	s.marty.phants@iqinc.com <s.marty.phants@iqinc.com>
9	2/20/2006	10:50:55	5	Print job	Test Page	Administrator	comp-normal	I/O-success		
10	2/20/2006	12:18:12	2	System Shutdown	WCP255	UTU100000N				
11	2/20/2006	12:21:01	1	System Startup	WCP255	UTU100000N				
12	2/20/2006	12:22:08	5	Print job	XEROX.PS	System User	comp-normal	I/O-success		
13	2/21/2006	14:04:20	14	LAN Fax job	LAN Fax job 1	UTU100000N	comp-normal	I/O-success	1	555-555-5555

Additional Information

Xerox Customer Support welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA),
TTY 1-800-855-2880 or at http://www.xerox.com.

Other Tips about Xerox multifunction devices are available at the following URL: http://www.office.xerox.com/support/dctips/dctips.html.

THE DOCUMENT COMPANY
XEROX®