Security information

Océ TDS TCS TC Systems

océ

Canon
CANON GROUP

Copyright

Edition 2013-08

Trademarks

Océ, and its wide-format printing systems are registered trademarks of Océ.

Microsoft®, Windows®, Windows XP®, Windows XP® embedded, Windows Server® 2003, Windows® Vista™, Windows Server® 2008, Windows ® 7, Windows Embedded Standard® 2009 are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries.

Linux® is a registered trademark of Linus Torvalds.

McAfee is a registered trademark or trademark of McAfee, Inc. or its subsidiaries in the United States and other countries.

Symantec and Norton are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Products in this publication are referred to by their general trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks of their respective companies.

Contents

Chapter 1
Introduction

The Océ Security for Océ TDS, TCS, TC systems

Definition

At Océ, security is an integral part of system development, and the company is taking a proactive approach to the improvement of security-related issues. Océ is working to address security requirements across all of its digital document systems.

For its printing systems connected to the network, Océ strives to ensure the:

- Security of the system on the network

- Security of the data sent to the printers, with a focus on protecting sensitive documents from being captured by un-authorised persons

- Security of the configuration and data on the controller

System security, data security and security on the network

Faced with system vulnerabilities, viruses, worms and in order to maximise the protection of the Océ print systems from hackers and networking attacks, Océ has reinforced the security of the Océ systems by:

- Introducing the **Océ Security levels** to offer network security protection against virus / worm attacks or system vulnerabilities (on Windows Operating Systems).
  Once the Security Interface is activated, you can define the level of security according to your system needs. Notice that the higher level of security you set, the fewer printing and scanning functionalities you get.
- Protecting the system **roles and passwords**. The main network and system settings are protected against change. Only authorised users can configure or change these settings
- Regularly checking the relevance of Microsoft flaws and delivering **security patches** whenever it is necessary.
- Providing **OS and software protection mechanism**. The internal system software is protected against alteration
- Implementing **network protocols protection** features (by use of the Océ Security levels filtering or by configuring each network protocol for firewall filtering)
- Restricting the access to the printer to allowed stations only
- Allowing the installation of an **Antivirus** software on the Océ system controller
- Being compliant with IPv6 and then benefiting from IPv6 secured assets
- The **HTTPS** (HTTP over SSL) protocol to encrypt the submitted print data

Océ online resources

Introduction

[We advise that you visit our website regularly in order to take full advantage of all the available resources:]

- [Find the latest supplies from our Media Guide.]
- [Get support on your product and answers to your questions in the Océ Knowledgebase.]
- Keep up-to-date with the latest information on security, the downloads for your drivers, software, printers and related documentation.

Get the latest information on Security

Connect to the International Corporate Website:

[www.global.oce.com]

Open the security page: http://global.oce.com/support/security/default.aspx.

Océ Online Knowledge Base

Océ permanently develops a base of knowledge for its products.

You can access this knowledge base through the Support section of our website.

Describe your question or problem in the search field. Then, find the answer in the list of solutions or documents, ordered by relevancy.

"http://global.oce.com/products/wfps-drivers/support.aspx"

Overview of the security features for the Océ TDS/TCS/TC4 systems

Introduction

The following Océ TDS/TCS/TC4 sytems are equipped with security features:

- Océ TDS300
- Océ TDS320
- Océ TDS400
- Océ TDS450
- Océ TDS600 and TDS600 Premia class
- Océ TDS700
- Océ TDS750
- Océ TDS800
- Océ TDS860 (TDS800 Pro Series)
- Océ TCS300
- Océ TCS400
- Océ TCS500
- Océ TC4 scanner

Security features overview

Operating System	Windows XP Service Pack 2 or Windows XP Service Pack 3 (see below)
MS Security patches	Océ released patches (on http://global.oce.com)
Network protocols protection	3 Océ Security Levels
Firewall	Yes
Antivirus	Compatible with 2 Antivirus brands
IPv6	Yes for: Océ TCS300 1.6 and higher Océ TCS500 1.6 and higher Océ TDS450 1.6 and higher Océ TDS700 1.6 and higher Océ TDS750 Océ TC4 1.6 and higher
Data encryption	Yes - HTTPS protocol for printing available with Océ Print Ex–ec Workgroup
Data overwrite	E-shredding (Océ TDS750 1.2.2 and higher and Océ TC4 1.8.2 and higher)
Password protection	Yes for configuration settings (in the Océ Settings Editor or Océ Express Webtools)

Operating System embedded in the Océ TDS/TCS/TC systems

Océ TDS/TCS/TC release installed with Windows XP SP3	Océ TDS/TCS/TC release installed with Windows XP SP2
Océ TDS300 1.1.10 and higher Océ TDS320 1.0.10 and higer Océ TDS400 2.1.10 and higher Océ TDS450 3.6 and higher Océ TDS600 4.1.10 and higher Océ TDS700 1.6 and higher Océ TDS750 Océ TDS800 2.1.10 and higher Océ TDS860 1.0.10 and higher Océ TCS300 1.6 and higher Océ TCS400 2.2.10 and higher Océ TCS500 1.6 and higher Océ TC4 1.6 and higher	Océ TDS300 1.1.9 and lower Océ TDS320 1.0.9 and lower Océ TDS400 2.1.9 and lower Océ TDS450 3.4 and lower Océ TDS600 4.1.9 and lower Océ TDS700 1.3 and lower Océ TDS800 2.1.9 and lower Océ TDS860 1.0.9 and lower Océ TCS300 1.3 and lower Océ TCS400 2.2.9 and lower Océ TCS500 1.5 and lower Océ TC4 1.0.3 and lower

Chapter 2
System and Network security

Ports - Protocols

Applications, protocols and ports used on the Océ TDS/TCS/TC systems

Printing applications: security levels, ports and protocols used by the Océ systems

Application /Functionality	System	Supported security levels (x) and open port			Port used on the controller: protocol
		N*	M*	H*	
Océ Wide-format Printer Driver for Microsoft Windows (WPD or WPD2)	All Océ TDS and TCS systems (except Océ TC4)	x TCP 515 TCP 65200 TCP 80 TCP 139	x(1) TCP 515 TCP 65200 TCP 80	x(2) TCP 515	TCP 515: LPR TCP 65200: Océ back-channel(**) TCP 139: SMB TCP 80: HTTP (for advanced accounting)
	Starting from: - Océ TDS450 3.8.2 - Océ TCS300 1.8.2 - Océ TCS500 1.8.2 - Océ TDS700 1.8.2 - Océ TDS750 1.2.2	UDP 515	UDP 515	UDP 515	UDP 515: Océ protocol (for printer discovery)
Océ Adobe® PostScript® 3™ driver	All Océ TDS and TCS systems (except Océ TC4)	x TCP 515 TCP 139	x(3) TCP 515 TCP 139	x(3) TCP 515	TCP 515: LPR TCP 139: SMB
Océ Print Exec Workgroup	- Océ TCS400/ TCS500 - Océ TDS400/ TDS450/ TDS600/ TDS700/ TDS750/ TDS800/ TDS860	x TCP 80	x TCP 80		TCP 80: HTTP
Océ Print Exec Workgroup over SSL (HTTPS)	- Océ TDS400/ TDS450/ TDS600/ TDS700/ TDS750/ TDS800/ TDS860, Océ TCS400/ TCS500	x TCP 443			TCP 443: HTTPS
	Starting from: - Océ TDS450 3.8.2 - Océ TCS500 1.8.2 - Océ TDS700 1.8.2 - Océ TDS750 1.2.2	TCP 443	TCP 443		

Application /Functionality	System	Supported security levels (x) and open port			Port used on the controller: protocol
		N*	M*	H*	
Océ Publisher Select	Océ TDS750 Océ TCS500	x TCP 515 TCP 65200 TCP 80 UDP 515	x TCP 515 TCP 65200 TCP 80		TCP 80: HTTP TCP 65200: Océ back-channel(*) TCP 515: LPR UDP 515: Océ protocol (for printer discovery)
Océ Publisher Mobile	All Océ TDS and TCS systems (except Océ TC4)	x TCP 21 TCP 4242 ICMP UDP 515			TCP 21: FTP TCP 4242: FTP passive mode(6) ICMP: ping UDP 515: Océ protocol (for printer discovery)
Océ ReproDesk	All Océ TDS and TCS systems (except Océ TC4)	x TCP 515 TCP 65200	x TCP 515 TCP 65200		TCP 515: LPR TCP 65200: Océ back-channel
Océ PELT Windows	All Océ TDS and TCS systems (except Océ TC4 and TDS750)	x TCP 515 TCP 65200	x TCP 515 TCP 65200	x(4) TCP 515	TCP 515: LPR TCP 65200: Océ back-channel
Océ Print Exec Light Web	Océ TDS400 1.X, Océ TDS600 2.X, Océ TDS800 1.X, Océ TCS400 <= 2.1	x TCP 80	x TCP 80		TCP 80: HTTP
Océ Print Exec Basic	All Océ TDS and TCS systems (except Océ TDS300 Océ TDS320, Océ TCS300 and Océ TC4)	x TCP 80	x TCP 80		TCP 80: HTTP
Novell NDPS printing	All Océ TDS and TCS systems (except Océ TC4)	x TCP 515	x TCP 515	x TCP 515	TCP 515: LPR
LPR printing (command line)	All Océ TDS and TCS systems (except Océ TC4)	x TCP 515	x TCP 515	x TCP 515	TCP 515: LPR
FTP printing	All Océ TDS and TCS systems (except Océ TC4)	x TCP 21 TCP 4242	x(5) TCP 21		TCP 21: FTP TCP 4242: FTP passive mode (6)

Application /Function–ality	System	Supported security lev–els (x) and open port			Port used on the controller: protocol
		N*	M*	H*	
SMB printing	- Océ TDS300/ TDS320/ TDS400/ TDS600/ TDS800/ TDS860 - Océ TCS400	x TCP 139			TCP 139: SMB

Notes:

- * Levels: N: Normal - M: Medium - H: High
- (**) Océ back-channel is an Océ proprietary protocol used to retrieve information from the printer (status, media loaded...) and to display it in the application or driver.
- (1) LPR printing with back-channel and advanced accounting. No SMB printing
- (2) LPR printing. No back-channel. No SMB printing. No advanced accounting
- (3) LPR printing only. No SMB printing
- (4) LPR printing. No back-channel
- (5) FTP active mode only
- (6) For FTP data communication channel

Scanning applications: security levels, ports and protocols used by the Océ systems

Application /Function–ality	System	Supported security lev–els (x) and open port			Port used on the controller: protocol
		N*	M*	H*	
Scan to File Remote SMB	All Océ TDS, TCS and TC4 systems except Océ TCS300 and Océ TDS300	x			SMB (no incoming port required on the controller)
Scan to File Remote FTP	All Océ TDS, TCS and TC4 systems except Océ TCS300 and Océ TDS300	x	x(1)	x(1)	FTP
Scan data retrieval by FTP	All Océ TDS, TCS and TC4 systems	x TCP 21 TCP 4242	x(2) TCP 21		TCP 21: FTP TCP 4242: FTP pas–sive mode (3)

Notes:

- * Levels: N: Normal - M: Medium - H: High
- (1) FTP passive mode only: the FTP server on the remote workstation must support FTP passive mode
- (2) FTP active mode only
- (3) For FTP data communication channel

Control management: security levels, ports and protocols used by the Océ systems

Application /Functionality	System	Supported security levels (x) and open port			Port used on the controller: protocol
		N*	M*	H*	
PING	All Océ TDS, TCS and TC4 systems	x	x	x	ICMP
SNMP based applications	Océ TDS450 v3.1 and higher	x UDP 161			UDP 161: SNMP
Océ Remote Logic	All Océ TDS and TCS systems except Océ TDS700, Océ TDS750, Océ TCS300 and Océ TC4	x TCP 1099 TCP 9999 TCP 16440 to TCP 16460			TCP 1099 TCP 9999 TCP 16440 to TCP16460 Océ specific protocol
Océ Power Logic Remote	Océ TDS700, Océ TDS750 and Océ TC4	x TCP 1099 TCP 9999 TCP 16440			TCP 1099 TCP 9999 TCP 16440 Océ specific protocol
Océ Settings Editor Web application	Océ TCS300	x TCP 80	x TCP 80		TCP 80: HTTP
Name resolution(**)	All Océ TDS, TCS and TC4 systems	x			Outgoing connection: - local port (on controller): UDP(/TCP) <dynamic value> - remote port (on DNS server): UDP(/TCP) 53
DHCP	All Océ TDS, TCS and TC4 systems	x	x	x	Outgoing connection: - local port (on controller) : UDP 68 - remote port (on DNS server): UDP 67
Océ Account Center Advanced accounting (WPD)	All Océ TDS, TCS and TC4 systems except Océ TCS300, Océ TDS300 and Océ TDS320	x TCP 80	x TCP 80		TCP 80: HTTP

Application /Functionality	System	Supported security levels (x) and open port			Port used on the controller: protocol
		N*	M*	H*	
Accounting information retrieval by FTP	All Océ TDS, TCS and TC4 systems except Océ TCS300, Océ TDS300 and Océ TDS320	x TCP 21 TCP 4242	x[1] TCP 21		TCP 21: FTP TCP 4242: FTP passive mode [3]
Browse Océ systems on the network with Windows network neighbourhood	Océ TDS450/ TDS700/ TDS750/ TC4 Océ TCS300/ TCS500	x UDP 137			UDP 137: NetBios over TCP/IP
Browse Océ systems on the network with Windows network neighbourhood	Océ TDS300/ TDS320/ TDS400/ TDS600/ TDS800/ TDS860 Océ TCS400	x UDP 137			UDP 137: SMB
Océ License Logic	All Océ TDS, TCS and TC4 systems	x TCP 80	x TCP 80		TCP 80: HTTP
Océ Remote Patch	All Océ TDS, TCS and TC4 systems except Océ TCS300	x TCP 80	x TCP 80		TCP 80: HTTP
Océ Remote Security settings	All Océ TDS and TCS systems except Océ TCS300, Océ TDS300, Océ TDS320 and Océ TC4	x TCP 80 TCP 443	x TCP 80		TCP 80: HTTP [3] TCP 443: HTTPS
	Starting from: - Océ TDS450 3.8.2 - Océ TCS500 1.8.2 - Océ TDS700 1.8.2 - Océ TDS750 1.2.2	TCP 80 TCP 443	TCP 80 TCP 443		
Océ Service Logic	All Océ TDS, TCS and TC4 systems	x TCP 21 TCP 4242	x[1] TCP 21		TCP 21: FTP TCP 4242: FTP passive mode [4]
Océ Meter Manager	Océ TDS450 1.7.1/ TDS700 1.7.1 and higher versions Océ TDS750 Océ TCS300 1.7.1/ TCS500 1.7.1 and higher versions	x UDP 161			UDP 161: SNMP

Notes:

- * Levels: N: Normal - M: Medium - H: High
- [**] The name resolution is mainly used to determine the IP address of the scan destination during Scan fo File operation
- [1] FTP active mode only
- [3] HTTP traffic is automatically redirected to HTTPS

- (4) For FTP data communication channel

Security Patches

Policy about Microsoft flaws and vulnerabilities

Policy

Océ regularly checks whether vulnerabilities (mainly described in the Microsoft security bulletins) affect the Océ Power Logic Controller. Then Océ informs the users whether the systems are vulnerable (or not), and in case of vulnerability, publishes a corresponding Océ Patch.

Patch procedure

Download the patches to apply to your printer from the http://global.oce.com website:

Select your print system and open the Downloads/security page (example: http://global.oce.com/products/tds700/Downloads.aspx#tab3) to get the latest patches and to check whether a Microsoft flaw impacts the Océ controller. On this page you find:

- The latest information about security (MS flaws...)
- The Océ security patches
- The instructions to apply the patches on the Océ controller
- The procedure to identify the Océ patches installed on your system

NOTE
The patches provided by Microsoft on the Microsoft website cannot be directly installed on the controllers. Use the appropriate Océ patches.

Consult also the Océ Security Web page - http://global.oce.com/support/security/ for general security information.

Depending on the version of your system controller, you must download the Océ Remote Patch and install it on the controller (see *Install the Océ Remote Patch™ - Remotely install an Océ patch* on page 21).

Install the Océ Remote Patch™ - Remotely install an Océ patch

Purpose

The Océ Remote Patch™ functionality allows you to:
- load and remotely apply Security and software patches onto the controller
- check the last patch successfully applied
- check the execution status of the latest patch applied ('Success' or 'Failure')

It is available for the following products versions:
- Océ TDS300 1.1.9 and higher
- Océ TDS320 1.0.9 and higher
- Océ TDS400 2.1.9 and higher
- Océ TDS450 3.3.1 and higher
- Océ TDS600 4.1.9 and higher
- Océ TDS700 1.2.1 and higher
- Océ TDS750
- Océ TDS800 2.1.9 and higher
- Océ TDS860 1.0.9 and higher
- Océ TCS400 2.2.9 and higher
- Océ TCS500 1.4.1 and higher
- Océ TC4 scanner 1.0.2 and higher

When to do

Each time a security patch needs to be remotely installed on the controller.

Before you begin

- Download the security patch from the Océ website (Downloads/Security page of your product on http://global.oce.com)

Open the Océ Remote Patch page either:

- in the web browser of a workstation: enter the URL http://[controller hostname or IPaddress]/OceRemotePatch.html

or

- In Océ Print Exec Workgroup v2.6 and higher: from the [Administration] menu, click Océ Remote Patch™

Log on to the Océ Remote Patch™ page as the controller system administrator.

Procedure

1. Browse to the location of the patch file(*.oce)

NOTE
Click 'Reset' to clear the field when needed

2. Click 'Apply Patch'
3. Confirm
   The installation starts. At the end of the process, the controller reboots.
4. After the restart:
   - in the web browser of a workstation enter the following URL: http://[controller hostname or IPaddress]/OceRemotePatch.html
   or

- from the [Administration] menu of Océ Print Exec Workgroup, click 'Océ Remote Patch™'

5. Log on as the controller system administrator
6. Check that the 'Last execution status' of the patch is 'Success': the installation was successful.

NOTE

When the status is 'Failure', apply the patch again.
If the installation fails again, contact your Océ representative.

Security levels

Security levels presentation

Introduction

Océ defined 3 levels of security according to the customer needs. The presentation below can help you to select the most suitable level.

HIGH security level

The HIGH level is the most secure mode for printing and scanning. The compliant applications are based on the LPR protocol for printing and on the FTP protocol for scanning.

Target:

- This level provides you with the most secure mode while using the basic feature for printing and scanning. Only some Océ applications are available. See the *security levels supported per application/functionality* on page 14.
- This security level may also be used when you want to be protected whenever a vulnerability has been discovered and the corresponding patch cannot be yet installed. As soon as the patch can be installed, you can go back to the original security level.

MEDIUM security level

The MEDIUM level is compliant with all the Océ applications available for printing and scanning which do not present a high risk (as reported by most popular network scanners).

Target:

This level is recommended if you need to be secured while you want to use the Océ applications for printing and/or scanning (you can use the system including more functions than with the HIGH security level).

Normal security level

This mode offers all the functionalities.

Target:

- You can select this level if you want to use some features not covered by MEDIUM security level.
- This level is more dedicated for small network infrastructure where security is less required versus features.

Security levels - Printers and scanner versions compatibility

Introduction

The security levels are implemented on the following versions of the printers/scanner controller:

Printers versions

Océ TDS300	v1.1.1 and higher
Océ TDS320	All versions
Océ TDS400	v2.1.1 and higher
Océ TDS450	All versions
Océ TDS600	v4.1.1 and higher
Océ TDS700	All versions
Océ TDS750	All versions
Océ TDS800	v2.1.1 and higher
Océ TDS860	v1.0 and higher
Océ TCS300	All versions
Océ TCS400	v2.2 and higher
Océ TCS500	All versions
Océ TC4 scanner	All versions

To check whether your Océ system **with no screen** is equipped, check the firmware version number on the control panel during the reboot of the printer.

For the Océ TDS300, the version number must be 1.1 or higher.

For the Océ TDS400, the version number must be 2.1 or higher.

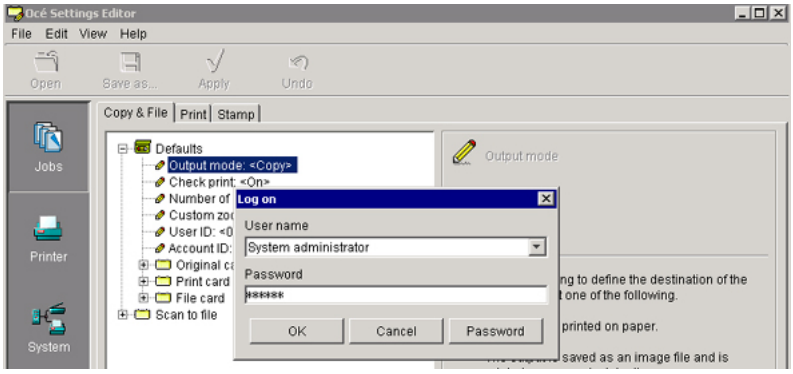
For the Océ TCS400, the version number must be 2.2 or higher (you can access it when the printer is off-line, on the 'Configure system' menu).

Set the Security level

Introduction

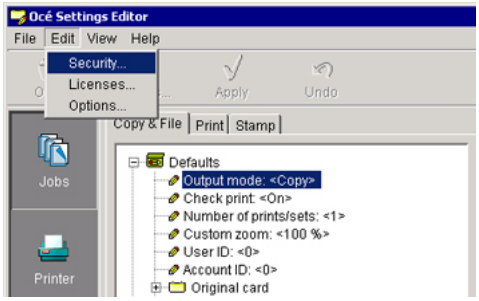
The security user interface is available locally on the controller only, from the Océ Settings Editor (no remote access).

NOTE
You need to be logged on as the System Administrator to access the security level interface and change the security levels.



[1] Log on

From the [Edit] menu, select [Security...] to open the [Security level] window.



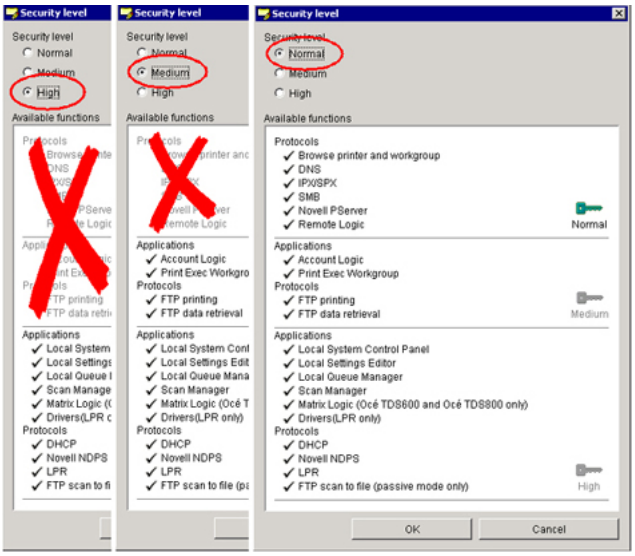
[2] Access Security window

It displays the current [Security level] and the available options.

According to the security level selected, the settings are available (in black) or not (in grey):

The controller is delivered with the [Normal] security level by default, but according to your needs, you can switch by selecting the required level.

Illustration

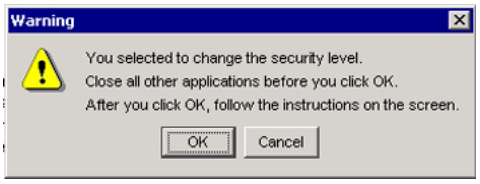


[3] Security level interfaces: High / Medium / Normal

Manage the security levels

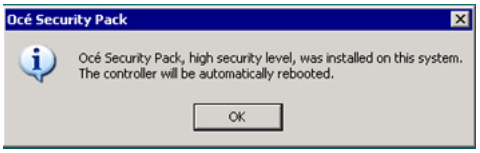
Procedure

1. In the [Security level] window, check the level required ([Normal], [Medium] or [High]).
2. Click [OK] once, then [Cancel]. A warning message is displayed:



[4] Security warning message

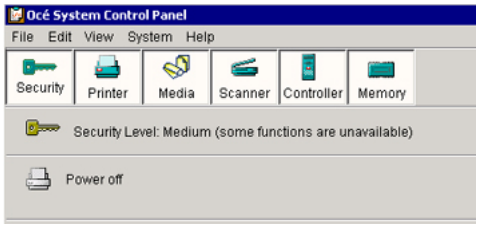
3. Click [OK].
4. After processing, a message displays the security level confirmation. Click [OK] to reboot the controller:



[5] reboot

Result

When the security level is changed from [Normal] to [Medium] or [High], the level selected is also displayed on the Océ System Control Panel (click on the [Security] button):



[6] Océ System Control Panel - Security level information

Systems with no screen

For systems delivered without screen, keyboard nor mouse, it is possible to switch between security levels using diskettes/CD.

There is one diskette/CD per security level:

- 1 diskette/CD to switch to HIGH security level.
- 1 diskette/CD to switch to MEDIUM security level.
- 1 diskette/CD to switch to STANDARD / Normal security level.

Océ delivers 3 deliverables to build the diskettes/CDs.

Please contact your local Océ representative.

Antivirus

Antivirus installation: Compatibility and recommendations

Introduction

To install the Symantec or MacAfee antivirus programmes, contact your Océ representative.

NOTE
Océ shall not be liable for damages of any kind attributable to the use of an antivirus on the Océ systems controllers.

Compatibility

Océ tested the installation of the 3 following antivirus programmes on the Océ systems controller:

Antivirus	installable on the controller of:
Symantec AntiVirus Endpoint Protection 11	• Océ TDS300 1.1.8.1 and upper • Océ TDS320 1.0.8.1 and upper • Océ TDS400 2.1.8.1 and upper • Océ TDS450 3.3.1 and upper • Océ TDS600 4.1.8.1 and upper • Océ TDS700 1.2.1 and upper • Océ TDS750 • Océ TDS800 2.1.8.1 and upper • Océ TDS860 1.0.8.1 and upper • Océ TCS300 1.2.1 and upper • Océ TCS400 2.2.6 and upper • Océ TCS500 1.4.1 and upper • Océ TC4 scanner 1.0.2 and upper
McAfee VirusScan Enterprise Edition 8.7i ePolicy Orchestrator for AntiVirus update	
Symantec AntiVirus Corporate Edition 10 (Norton)	• Océ TDS300 1.1.3 to 1.1.5 • Océ TDS320 • Océ TDS400 2.1.3 and upper • Océ TDS450 • Océ TDS600 4.1.3 and upper • Océ TDS700 • Océ TDS750 • Océ TDS800 2.1.3 and upper • Océ TDS860 1.0.1 and upper • Océ TCS300 • Océ TCS400 2.2.2 and upper • Océ TCS500 • Océ TC4 scanner

Roles and Passwords

Roles and Passwords for the Océ TDS/TCS/TC4 systems (except Océ TCS300)

Roles

In all Océ TDS/TCS/TC4 (except TCS300) systems, the main network and system settings are protected against change. Only authorised users can configure or change these settings.

4 roles are available:

- Key operator:
  The Key Operator can manage the jobs and the device settings
- Repro operator
  The Repro operator can manage jobs (print and scan)
- System administrator
  The System Administrator can manage the Configuration settings (such as the Network settings, scan destinations settings...) and print jobs
- Océ service
  This role is used exclusively by the Océ Service Technician

NOTE
Refer to your Océ TDS/TCS/TC4 user manual to get information related to the authorised users and to the settings access rights.

Passwords used

The passwords protect:

- The roles
- The Scan To file remote user name

Password modification table for Océ TDS/TCS/TC4 systems

Password for	Can be changed by
Key operator	Key operator
Repro operator	Repro operator
System administrator	System administrator
ScanToFile remote user name	Anyone (no login requested)

NOTE
Keep these passwords. The loss of these passwords may require the intervention of Océ Service.

Passwords storage on the controller

All passwords are stored encrypted on the controller. There is no open access to the system to change them.

You can change them only through the standard user interface on the controller.

Passwords export policy

No password is exported to the backup files, except the passwords for the Scan To File remote user names.

The passwords for the Scan To File remote user names are stored encrypted (in the *.sm file)

Roles and Passwords for the Océ TCS300

Roles description

In the system, the main network and system settings are protected against change. Only authorised users can configure/change these settings.

4 roles are available:

- Key operator:
  The Key Operator can manage the jobs and the device settings
- System administrator
  The System Administrator can manage the Configuration settings such as the Network settings and the scan destinations settings
- Power user
  The Power User has both the rights of the Key Operator and the System Administrator
- Océ service
  This role is used exclusively by the Océ Service Technician

Passwords used in Océ Settings Editor Web application

In Océ Océ Settings Editor Web application the passwords protect the roles.

Password modification table for Océ TCS300

Password for	Can be changed by
Key operator	Key operator or Power user
System administrator	System administrator or Power user
Power user	Power user

Password policy

- 256 characters maximum
- Any number [0-9]
- Any letter lowercase/uppercase [a-z][A-Z]
- the following special characters:

_	-	~	!	@	#	$	%	^	*	?	{	}
(	)	=	+	,	.	;	:	[	]	/	|	\

Passwords storage on the controller

All passwords are stored encrypted on the controller. There is no open access to the system to change them.

You can change them only through the standard user interface on the controller.

Passwords export policy

The roles passwords are not stored in the backup set.

Chapter 3
Data security

HTTPS through PEWG

Print data encryption through HTTPS with Océ Print Exec Workgroup

Introduction

To protect the privacy of your print data on the network, use the HTTPS protocol (HTTP over SSL) with Océ Print Exec Workgroup (v2.6 and higher).

You can then send encrypted print data to Print Exec Workgroup using the following URL:

https://[Common Name or PrinterHostname or PrinterIPaddress]

Example: https://TCS500.oce.com

Definition

Océ proposes 2 services when printing with Print Exec Workgroup by means of HTTPS instead of HTTP:

- the print data encryption to ensure the print data confidentiality
- the use of certificates: the client station which submits the print can check the identity of the controller.

Compatible versions of Océ Print Exec Workgroup

The HTTPS feature is embedded in Océ Print Exec Workgroup v2.6 and higher, recommended for :

- Océ TDS400
- Océ TDS400 Prémia Class
- Océ TDS450
- Océ TDS600
- Océ TDS600 Premia Class
- Océ TDS700
- Océ TDS750
- Océ TDS800
- Océ TDS800 Pro series
- Océ TCS400
- Océ TCS500

The self-signed certificate and the CA-signed certificate

- By default, Océ delivers an Océ self-signed certificate. This certificate provides encryption of the print data between the client and the controller. It can be easily used.
  This self-signed certificate has not been signed by a Certification Authority, consequently the web browser will display a 'Certificate Error' message the first time you use the HTTPS protocol.
  This certificate may be used with a few limitations (see *Use the Océ self-signed certificate with Internet Explorer* on page 37) or while you are waiting for a trusted certificate to be delivered by a Certification Authority.
- When your security policy recommends it, the administrator can request and import a certificate delivered by a Certification Authority (CA-signed certificate).
  See the *overall procedure to request and import a CA-signed certificate* on page 41.

HTTPS protocol and the Security levels

The HTTPS protocol in Océ Print Exec Workgroup is available only in Normal security level.

The HTTPS protocol uses the TCP port 443.

Administration

Configure the use of HTTPS

Introduction

You can configure the use of HTTPS through the job submission tool for Océ TDS and TCS systems: Océ Print Exec Workgroup v2.6 and higher.

On the Remote Security™ page, set the use of the secured protocol to:

- [Required] to allow only HTTPS protocol

- [Optional] to allow both HTTP and HTTPS protocols

NOTE
When you set HTTPS to 'required' in PEWG v2.6 or higher, only the Océ Account Center communication protocol remains in HTTP mode.

Configure the use of HTTPS

Procedure

1. In a web browser, open Océ Print Exec Workgroup v 2.6 or higher (enter the printer IP address or hostname)
2. From the Administration menu, select Océ Remote Security
3. Log on as the printer system administrator
4. On the Océ Remote Security™ page, select [Set the HTTPS mode]
5. Set the HTTPS mode to [Required] or keep [Optional] (default)
6. [Reboot the controller to apply the change]

Use the Océ self-signed certificate

Introduction

You can use the HTTPS protocol with the default Océ self-signed certificate to send encrypted print data to the printer controller.

The first time you use a self-signed certificate, your web browser will generate security error messages.

In order to easily and securely use the self-signed certificate in your web browser, you must:

- View and check the self-signed certificate in your web browser

- Configure your web browser to trust the self-signed certificate

The procedures depend on the web browser you use to open Océ Print Exec Workgroup. See below the use with:

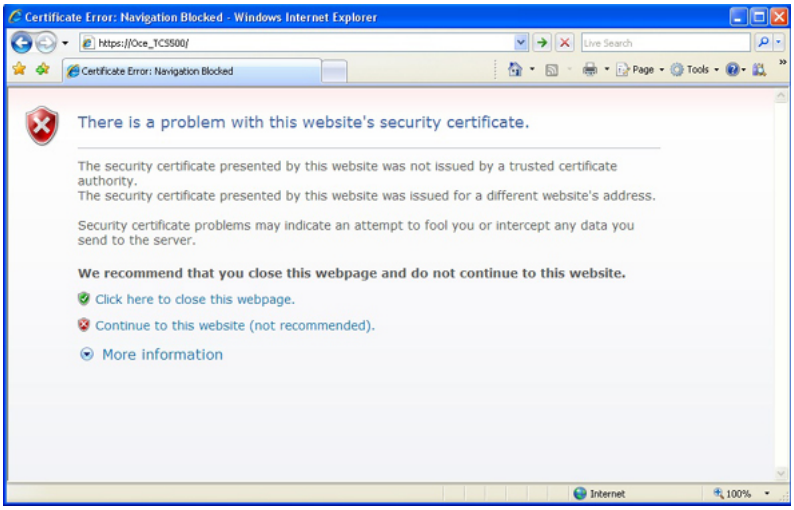
- Internet Explorer

- Mozilla Firefox

Use the Océ self-signed certificate with Internet Explorer

Procedure

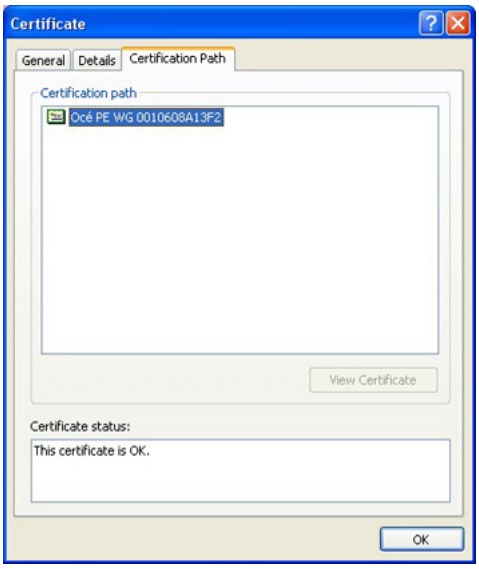
1. On a workstation, type the URL address of your printer in Internet Explorer (https://[hostname]).
   A warning window opens. It displays 2 errors:
   - The certificate is not issued by a trusted certificate authority.
   - The Common Name in the certificate does not match the printer hostname (or IP Address) you typed in the address bar.



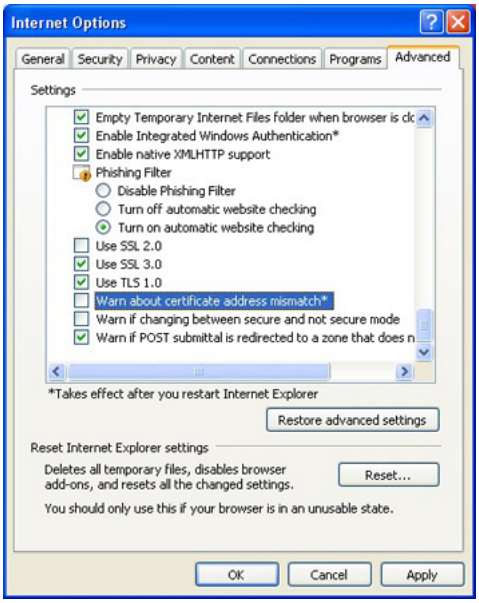
2. In order to view and check the self-signed certificate, continue to the website.

NOTE
A warning- Security message may open to ask whether you trust the applet distributed by Océ. This message concerns only the Java applets used in Print Exec Workgroup. It is not related to the self-signed certificate.
You can check the certificate and click 'Yes'.

3. Océ Print Exec Workgroup opens, but the address bar displays a certificate error. Click on the error.
   The certificate is invalid.
4. View the certificate.
5. The certificate is issued to 'Océ PE WG xxxxxxxx' by 'Océ PE WG xxxxxxxx' (where 'xxxxxxxx' is the controller Mac Address).
   Check the Details and the Certification Path.
   In Details, check the following values:
   Common Name (CN) = Océ PE WG
   Organization Unit (OU) = PE WG
   Organization (O) = Océ
6. Click 'Install Certificate...'
7. Follow the Wizard's instructions to import the certificate into your web browser.
   Validate.
   When the import is successful, the 'Océ PE WG' Certificate is recognised and its status is OK.



8. Open the Tools menu\Internet options\Advanced tab. In the Security section, uncheck the option "Warn about certificate address mismatch"



9. Restart the browser and type the URL of your printer in Internet Explorer (https://[hostname]).

Result

The padlock is displayed on the address bar, Océ self-signed certificate guarantees:
- The identity of the remote computer (controller)
- The encryption of the print data on the network.

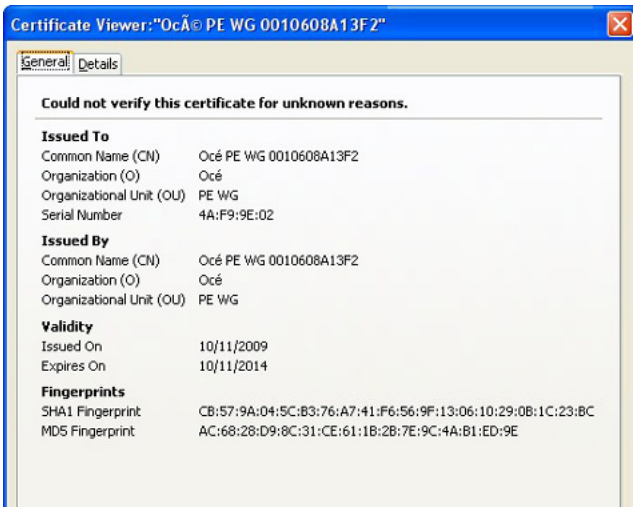
Use the Océ self-signed certificate with Mozilla Firefox

Procedure

1. On a workstation, type the URL address of your printer in Mozilla Firefox (https://[hostname]).
   A warning window opens. It displays 2 errors:
   - The certificate is not trusted because it is self-signed
   - The certificate is only valid for 'Océ PE WG xxxxxxxx'

2. In order to view and check the self-signed certificate, continue to add an exception.
3. Click 'Add Exception...'
4. In the 'Add Security Exception' window, click 'Get Certificate' to get the certificate from the controller web server.
   The 'Wrong site' and 'Unknown Identity' errors are displayed.

5. Click 'View...' to see the content of the certificate.
   Check the following values:
   Common Name (CN) = Océ PE WG xxxxxxxx
   Organization Unit (OU) = PE WG
   Organization (O) = Océ



6. The certificate is issued to 'Océ PE WG xxxxxxxxx' by 'Océ PE WG xxxxxxxx', so you can confirm the security exception (permanent or temporary exception).
7. A security warning window may pop-up. Click 'Yes' to continue.

Result

The Océ Print Exec Workgroup software opens.

You can check in the status bar (at the bottom of the window) that the padlock is displayed.

In the navigation bar, the Océ certificate is registered as an exception.

The identity of the remote controller and the encryption of the data on the network are secured.

Request and import a CA-signed certificate

Description of the overall procedure to request and import a CA-signed certificate

Introduction

By default the first certificate delivered for the use of HTTPS with Océ Print Exec Workgroup is an Océ self-signed certificate.

To ensure a fully trusted authentication, you can request and import a certificate delivered by a Certification Authority (CA-signed certificate).

Information about certificates

When you generate a CA-signed certificate request on a controller:

- A new private key is created: this key stays in the controller
- The certificate request containing the public key is created. Send it to the Certification Authority.
  The CA-signed certificate you will receive also contains the public key. This public key is linked to the private key already stored in the controller.

In the controller, the private key and the public key must match to enable a secure HTTPS protocol.

To request and then import a CA-signed certificate while you are still using HTTPS with Océ Print Exec Workgroup 2.6 and higher, follow these 2 procedures, step by step:

Overall procedure to prepare and generate the CA-signed certificate request (Océ Print Exec Workgroup 2.6 and higher)

Step	Description
A1- Back up the current certificate and private key	The current certificate can be: • the original Océ self-signed certificate embedded with Océ Print Exec Workgroup • a CA-signed certificate (delivered by a Certification Authority) you previously installed See *Back up a certificate and a private key* on page 43.
A2- Generate the certificate request	Make this step when you want to request and install a CA-signed certificate. During the creation of the request, a new private key is created. See *Generate a certificate request* on page 44.
A3- Save the content of the certifi–cate request	Send this content to the Certification Authority to re–quest a (CA-signed) certificate The Certification Authority will check the request and re–ply. - If the request is valid, go to step A4 - if the request is not valid, make a new request (A2) ac–cording to the remarks/corrections suggested by the CA request feedback

Step	Description
A4- Restart the controller	

Overall procedure to import the new CA-signed certificate

Step	Description
B1- Save and store the new CA-signed certificate	Save the CA-signed certificate you received from the Certification Authority.
B2- Import the new CA-signed certificate into the controller	Import the CA-signed certificate (Root and/or Intermediate and CA-signed certificates). See *Import a CA-signed certificate (into the controller and workstations)* on page 46
B3- Restart the controller	
B4- Import the Root certificate into the web browsers of the workstations	The Root certificate identifies the Certification Authority. By default, the web browsers contain a list of well-known and trusted Root certificates. In case the Root certificate of the Certification Authority is not in this list, install the CA Root certificate in the 'Trusted Root certificates' list of the web browser, on each workstation. See *Check and import the Root certificate into the workstations browser* on page 47
B5- Back up the certificate and private key	Back up and store the certificate and the private key in order to be able to restore them if needed. See *Back up a certificate and a private key* on page 43.

Back up a certificate and a private key

When to do

You must back up the certificate and private key:

- BEFORE you generate a certificate request (step A1 of the *overall procedure* on page 41):
  To save your current certificate and private key.
- AFTER you import the new certificate (step B5):
  To save your new certificate and private key, in order to be able to restore them if needed.

Back up the current certificate and private key

Procedure

1. In a web browser, open Océ Print Exec Workgroup v2.6 or higher (https:\\[IP address or hostname])
2. From the Administration menu, select Océ Remote Security
   A new HTTPS browser page opens.

NOTE
A warning message can occur: validate and continue.

3. Log on as the printer system administrator
4. On the Océ Remote Security™ page, select [Backup certificate and private key]
5. To save the server certificate and private key, enter a password made of 6 characters at least ([Password used to encrypt the private key])
6. Confirm the password
7. Click 'Save'
8. Download and store the back up file (.jks).

Generate a CA-signed certificate request

Purpose

Create a certificate request in Océ Print Exec Workgroup 2.6 and higher.

Use this function only when you want to request a new CA-certificate.

Pre-requisites

Install the latest version of Print Exec WorkGroup for your printer (v2.6 or higher, see http://global.oce.com/products/print-exec-workgroup/)

Back up the current Certificate and Private key already installed on the controller (see *Back up a certificate and a private key* on page 43).

[Generate a certificate request]

NOTE
Step A2 of the *overall procedure* on page 41.

Procedure

1. In a web browser, open Océ Print Exec Workgroup v 2.6 or higher (https:\\[IP address or hostname])
2. From the Administration menu, select Océ Remote Security
   A new HTTPS browser page opens.

NOTE
A warning message can occur: validate and continue.

3. Log on as the printer system administrator
4. On the Océ Remote Security™ page, select [Generate a certificate request]
5. Fill out the form with the requested information

NOTE
In the certificate request the Common Name MUST be the hostname or the Fully Qualified Domain Name (FQDN) of the printer (e.g.: or ''TDS800' or 'TDS800.mycompany.com').
This Common Name will be used in the URL when you open Océ Print Exec WorkGroup through HTTPS (e.g.: 'https://[CommonName]).

6. Click 'Generate'.

Result

The web server generates a certificate request. The content of the request is displayed (plain text).

Example (fake request):

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIBvDCCASQAwfDELMAkGA1UEBMCRlIxDDAKBgNVBAgTA0lERjEQMA4GA1UEBxMHQ1JFVEVJ

TDEBEGA1UEChMKT2NIIFBMVCBTQTEMMAoGA1UECxMDU05TMSowKAYDVQQDEyF0ZHM3MDAtNzQw

LnNucy5vY2VjcmV0WlsLm9jZS5uZwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ2NKQMd

HjiDZ1khzTJTORxHqjKl3AtE3PXqRsiHouTH5JTceYtaBjCnxCJ4pGKY5iKN8KJiJuZG8PHxY7o

W/+zpvxN2VtX7TcyTAvyCThUwL+cqo75tvODo5HMCUa2sLdl8GO9WMLpgZkxH5KzliO+Lcl4

yQbqhENynywS0C2ObXCq3yksF74+XlO0swhoA2yfDp4T+LuF3wxys8lUH3ZhhkOYg==

-----END NEW CERTIFICATE REQUEST-----

Save and send the request

When to do

NOTE
Step A3 of the *overall procedure* on page 41.

Procedure

1. Click 'Save' to save the content of the request in a .csr file (named 'certificate_request.csr' by default)
2. Restart the controller
3. Send the content of this request to the Certification Authority.

Import a CA-signed certificate (into the controller and workstations)

Introduction: overall procedure

1. Import the CA-signed certificate into the controller:
   - Import the 'Root certificate'
   - Import the 'Intermediate certificate'
   - Import the CA-certificate
2. Import the Root certificate into the workstations web browser

Import the [Root certificate] into the controller

NOTE
Step B2 of the *overall procedure* on page 41
Save locally or on the network all the CA-signed certificate files the Certification Authority sent you.

Procedure

1. In a web browser, open Océ Print Exec Workgroup v2.6 or higher (https:\\[IP address or hostname])
2. From the Administration menu, select Océ Remote Security
   A new HTTPS browser page opens.

NOTE
A warning message can occur: validate and continue.

3. Log on as the printer system administrator
4. On the Océ Remote Security™ page, select [Import CA-signed certificate]
5. Select [Root certificate]
6. Browse to the Root certificate file and click [Import]

NOTE
The Root certificate may already exist in the web server certificates list.

7. Validate to confirm the import
8. When the message [Certificate successfully imported.] pops up, go on to import the [Intermediate certificate]

NOTE
If an error message is displayed, see its meaning in *Security through PEWG 2.6 and higher: Error messages* on page 50.

Import the [Intermediate certificate]

Procedure

1. Select [Intermediate certificate]
2. Browse to the Intermediate certificate file and click [Import]
3. When the message [Certificate successfully imported.] pops up, go back to the main page to import the [CA-signed certificate]

Import the [CA-signed certificate]

Procedure

1. Select [CA-signed certificate]
2. Browse to the certificate file
3. Select 'Yes' to validate the certificate against Java root certificates and click 'Import'
4. When the message [Certificate successfully imported.] pops up, restart the controller.

Result

Result: The certificate is now installed on the server.

Check and import (if needed) the CA Root certificate also into the workstations web browser. That will secure the complete data workflow between the workstations and the server.

Check and import the [Root certificate] into the workstations browser

When to do

NOTE
Step B4 of the *overall procedure* on page 41

Procedure

1. On each workstation, open the web browser
2. In the Tools - Internet Options - Content window, open the 'Certificates'
3. Check if the CA [Root certificate] is already displayed in the 'Trusted Root Certification Authorities' list
4. If it is not in the list, import the CA Root certificate.

Restore a certificate and a private key

When to do

You can restore the certificate and the private key at any moment, in case of need.

Restore the certificate and private key

Procedure

1. In a web browser, open Océ Print Exec Workgroup v 2.6 or higher (https:\\[IP address or hostname])
2. From the Administration menu, select Océ Remote Security
   A new HTTPS browser page opens.

NOTE
A warning message can occur: validate and continue.

3. Log on as the printer system administrator
4. On the Océ Remote Security™ page, select [Restore certificate and private key]
5. Browse to the back up file
6. Enter the password of the back up file
7. Click 'Restore'
8. A dialog box opens: [This action will overwrite the current certificate. Continue?]
   Click 'OK'
9. When the key and the certificate are successfully restored, restart the controller.

Reset the current certificate

Purpose

This procedure creates a new Océ self-signed certificate.

When to do

You can reset the certificate after a certificate request or at any moment when you want to restore a self-signed certificate.

NOTE
Prefer the restoration of the original self-signed certificate (that requests a preliminary back up of the original self-signed certificate):
Each 'Reset certificate' action generates a new self-signed certificate (with a new private and public key). So each time you reset the certificate, you must import the new certificate into the web browser.

Reset the certificate

Procedure

1. In a web browser, open Océ Print Exec Workgroup v2.6 or higher (https:\\[IP address or hostname])
2. From the Administration menu, select Océ Remote Security
   A new HTTPS browser page opens.

NOTE
A warning message can occur: validate and continue.

3. Log on as the printer system administrator
4. On the Océ Remote Security™ page, select [Reset certificate]
5. Click the 'Reset' button
6. When the reset is successful ([Certificate successfully reset]), reboot the controller

Result

A new self-signed certificate has been generated on the controller.

Configure your web browser to use it (see *Use the Océ self-signed certificate with Internet Explorer* on page 37)

HTTPS and certificates error messages

Security through PEWG 2.6 and higher: Error messages

Introduction

Find below the description of the error messages you can encounter when you manage security through Print Exec Workgroup 2.6 and higher:

If the error message is:	That means:
'Incorrect Login' 'Administrator's session has expired'	Type in the correct login/password to open the Océ Remote Security page. The session expires after 5 minutes.
[Incorrect password]	Type the password used to back up the certifi–cate
[An internal server error occurred while pro–cessing the request. Repeat the operation]	• An internal error occurred during the gener–ation of the certificate request • An internal error occurred during the reset of the certificate • An internal error occurred during the resto–ration of the back up file Repeat the operation. If the operation fails again, contact your system administrator or your Océ local representative.
[Certificate import failed. Check the validity of the certificate file.]	The file you try to import is not a valid certifi–cate file.
[Error: This CA-signed certificate does not match the latest CA-signed certificate request.]	The certificate you try to import does not match the certificate request (Private key). Possible causes: • the imported certificate does not match the certificate request • the certificate has been reset (to a self-sign–ed one)
[The certificate chain cannot be established. Import Root and/or Intermediate certificates first.]	The controller does not recognise the Root or Intermediate certificate provided by the Certifi–cation Authority. Import the Root or/and the Intermediate certifi–cate in the controller before you import the certificate. (See *Import the Root certificate into the con–troller* on page 46 and *Import the Intermediate certificate* on page 46
[Certificate already imported]	The certificate has already been imported
[Error when saving file. Operation aborted.]	The back up process failed due to an internal error. Repeat the operation.

E-Shredding (Océ TDS750 1.2.2 and higher, Océ TC4 1.8.2 and higher)

E-shredding presentation

Introduction

The e-shredding feature is a security feature which allows to overwrite any user data (print/copy/scan) when it is deleted from the system.

This feature prevents the recovery of any deleted user data (files' content and attributes)

A deleted job is a job that cannot be retrieved from any user interface.

When is a job deleted?

A job is deleted either:

- When it is manually deleted from a Smart Inbox
- After it was successfully printed and was not saved in a Smart Inbox ('Save printed jobs in a Smart Inbox' system setting is disabled in the Océ Express Webtools)
- After a 'ScanToFile to remote destination' has been successfully performed
- When it is automatically deleted after a timeout:
  - When the end of the job lifetime in the Smart Inbox is reached ('Save printed jobs in a Smart Inbox' system setting is enabled in the Océ Express Webtools and the 'Printed jobs in Smart Inbox: job lifetime' is set)
  - When the time for the cleanup of the 'Scans in Smart Inbox' is reached
- When a 'Clear system Remove all jobs' is performed on the printer local interface

E-shredding algorithms

Select one of the three e-shredding behaviours:

- **DOD 5220.22-M**: 3-pass overwriting algorithm (compliant with the US Department of Defense directive):
- **Gutmann**: 35-pass overwriting algorithm with random data
- **Custom**: set the number of passes, from 1 to 35.

NOTE

The e-shredding feature has been designed to minimise impact of the global system performance.
However the more passes selected, the more impact it has on general performance.
It is recommended to minimise the number of passes when document production is required.

Enable the e-shredding on Océ TDS750 1.2.2 and higher and Océ TC4 1.8.2 and higher

Before you begin

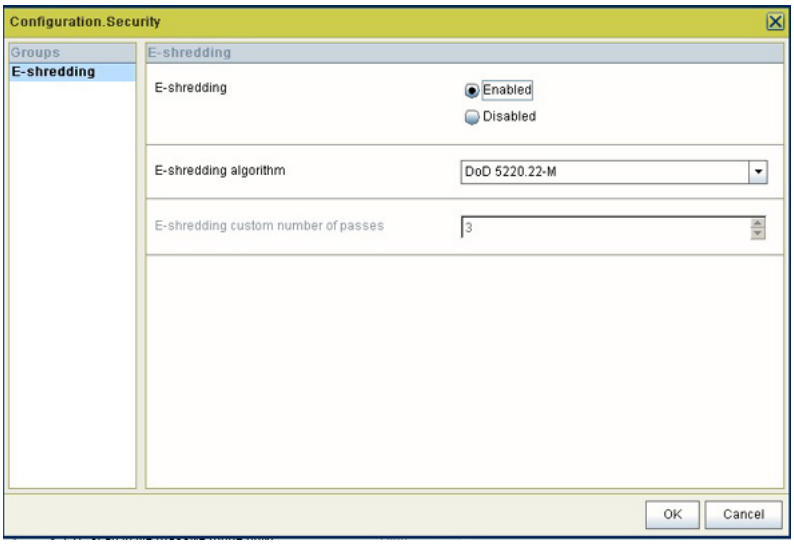
You must be logged as a System Administrator.

NOTE
When you enable the e-shredding, the system automatically disables the 'Save printed jobs in a Smart Inbox' setting. The jobs previously printed and stored in the Smart Inbox are deleted. They are not e-shredded.

Enable/disable the e-shredding (Océ Power Logic Controller)

Procedure

1. Open the system Océ Power Logic Controller
2. Open the 'Configuration' - 'Security' tab and go to the 'E-shredding' section
3. Log on as a System Administrator
4. Click Edit
5. Select 'Enabled'



6. Select the algorithm.
When you select 'Custom', set the number of passes

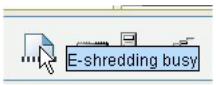
Result

When the E-shredding feature is enabled, a new icon is added to the list of icons (bottom right) in the Océ Power Logic Controller interface.

Each time data (file's content or attributes) is deleted from the system, the e-shredding process occurs.

For a while, the E-shredding feedback returns 'busy'.

In the Océ Power Logic Controller interface, roll the mouse over the e-shredding icon to display the 'E-shredding busy' status



Once the e-shredding data process is complete, the status comes back to 'E-shredding ready' in the Océ Power Logic Controller interface (roll over the icon).

NOTE

In case some scanned files have a 'Scan destination file name' composed of more than 256 characters, on the controller or on the remote destination, they will be deleted, but they will not be e-shredded (too long filename).

E-shredding process and system behaviour in Océ TDS750 1.2.2 and higher and Océ TC4 1.8.2 and higher

When you enable the e-shredding

When you enable the e-shredding, the system starts the e-shredding process for all scan/copy/print jobs that will be deleted.

E-shredding process will occur as a background task.

All processed jobs will be e-shredded after they are deleted:

- After a manual deletion from the 'Waiting jobs'

- After an automatic deletion of the print and scan jobs by the system

NOTE
On TC4 systems, all jobs processed by Océ Publisher Copy are not e-shredded after deletion.

When you disable the e-shredding

When you disable the e-shredding, the system:
- Terminates the e-shredding process for files which are being e-shredded
- Will not e-shred the new deleted files

Make sure all the scan/copy/print jobs are completely e-shredded

Once a batch of scan/copy/print jobs has been processed, perform the following actions to make sure all the files are e-shredded:

1- Unplug the system from the network

2- Check that 'Enable Printed jobs' is set to 'Off' (Océ TDS750 only)

3- Delete any print jobs from the 'Waiting Jobs' (TDS750), and any scan jobs from the controller

4- In the top menu, open 'System'

5- Select 'Clear System'

6- Wait until the e-shredder status comes back to 'Ready'

7- Restart the system

8- Wait until the e-shredder status displays 'Ready'

Index

CANON INC.
www.canon.com

CANON U.S.A., INC.
www.usa.canon.com

CANON CANADA, INC.
www.canon.ca

CANON EUROPA INC.
www.canon-europe.com

CANON LATIN AMERICA INC.
ww.cla.canon.com

CANON AUSTRALIA PTY. LTD
www.canon.com.au

CANON CHINA CO., LTD
www.canon.com.cn

CANON SINGAPORE PTE. LTD.
www.canon.com.sg

CANON HONGKONG CO., LTD
www.canon.com.hk