Océ User manual

Océ VarioPrint® 2045-65,
Océ VarioPrint® 2050-70,
Océ 31x5

Common Criteria certified configuration of the DAC R8.1.10

Océ-Technologies B.V.

Edition 2005-10

Contents

Chapter 1
General information

About the DAC release 8.1.10

Introduction

The DAC (Digital Access Controller) release 8.1.10 is the controller for print and scan jobs used with the following Océ products:

- Océ VarioPrint® 2050, 2060 and 2070.
- Océ VarioPrint® 2045, 2055 and 2065.
- Océ 3145, 3155 and 3165.

The DAC (Digital Access Controller) release 8.1.10 will be referred to as DAC in this manual.

This manual is intended for the System administrators that deploy and administer the DAC in the certified configuration. When information in this (Common Criteria certified configuration of the DAC R8.1.10) document differs from any other documentation about administering the DAC in the certified configuration, only the information in this document is valid.

The DAC is intended to provide scan and print functionality to users requiring a low to moderate level of security assurance (Common Criteria Evaluation Assurance Level 2+).

Security functions

The following security functions are evaluated to meet the Common Criteria Evaluation Assurance Level 2+:

- E-Shredding (automatic data overwriting).
- Secured printing (protect print jobs with a PIN).
- IP filtering (built-in firewall).
- Security management functions.
- Self test (integrity check with auto-repair).

Additional information

For details refer to the DAC Security Target document BSI-DSZ-CC-0325 on the following web sites:

- www.oce.com
- www.commoncriteriaportal.org
- www.bsi.de

Assumptions

Introduction

The following assumpions focus on the organisation where the Océ product and the DAC is located and describe the environment, the security policy, the users and their behaviour.

Océ products

It is assumed that the DAC is attached to an:

- Océ VarioPrint® 2050, 2060 or 2070 machine, or
- Océ VarioPrint® 2045, 2055 or 2065 machine, or
- Océ 3145, 3155 or 3165 machine.

Security policy

It is assumed that the organisation will have a security policy governing the use of IT products by employees in the organisation.

The security policy describes and requires a low to medium level of assurance (Common Criteria Evaluation Assurance Level 2) for the DAC.

It is assumed that the network to which the DAC is attached is protected by security measures that are intended to prevent malicious programs, viruses and network traffic, not related to the working of the operational environment, entering the network to which it is attached. Although the virus database files and various patches are kept up to date, the policy recognises that new threats emerge over time and that occasionally they may enter the environment from outside and provides measures to help limit the damage. The policy will define how IT products are protected against threats originating from outside the organisation.

The employees of the organisation are aware of, are trained in and operate according to the terms and conditions of the policy. The policy also covers physical security and the need for employees to work in a security aware manner including the usage of the DAC.

Environment

It is assumed that the operational environment of the DAC is a regular office environment. Physical access to the operational environment is restricted. The environment contains non-threatening office personnel (local users, remote users, remote system administrator, Océ service engineer). A “thief” is only rarely present in this environment and not on a recurring base.

Remote System administrator

It is assumed that the DAC is used in the security mode 'High (factory default)'. The security mode will not be changed.

The remote System administrator will read the available System administrator documentation and must be aware of the security policy of the organisation. The remote System administrator has to work in a security aware manner with the DAC.

Local and remote users

When secure print jobs are sent to the DAC, the user will specify a PIN of at least 4 digits and a maximum of 6 digits and, whether the job is printed or not, will delete the job on the same working day. Employees are aware of this requirement.

The user will read the available user documentation and must be aware of the security policy of the organisation. The user has to work in a security aware manner with the DAC.

E-shredding

It is assumed that the E-shredding operation for print jobs and scan job data objects will not be disabled.

Chapter 2
DAC Configuration

Océ System Configuration

Introduction

The Océ System Configuration application enables the remote System administrator to configure and administer the DAC via a HTTPs connection.

Note: *The DAC needs an operational TCP/IP network connection before Océ System Configuration can be used. To check the configuration, use the Key Operator System (KOS) of the machine to print a configuration report. To configure the IP address settings of the DAC, use the Key Operator System (KOS) of the machine. To learn how to use the Key Operator System (KOS), see the Configuration and maintenance manual. You can download the manual at www.oce.com.*

Attention: The remote System administrator must not change the security mode. Otherwise the DAC is no longer in the certified configuration and is no longer able to assure the security of its objects and itself. It is not possible to get the DAC back into the certified configuration by changing the security mode back to 'High'.

Attention: The remote System administrator must not change the 'Jobs to overwrite' settings. If E-shredding is disabled for 'scan jobs' or 'print jobs without security code', the DAC is no longer in the certified configuration and is no longer able to assure the security of 'scan jobs' and 'print jobs without security code'.

Secure connection

The network HTTPs connection to the Océ System Configuration application is protected with SSL (Secure Socket Layer).

For the purpose of configuring the DAC prior to deployment, the DAC is delivered with a factory-default SSL certificate. A new SSL certificate should be created before the DAC is deployed. This must be done after the hostname of the DAC is configured.

Authentication

The Océ System Configuration application is password protected.

For the purpose of configuring the DAC prior to deployment, the DAC is delivered with a factory-default password. The remote System administrator must change the password before the DAC is deployed.

The remote System administrator must not use a short or easy-to-guess password. Use a non-predictable sequence of at least 5 characters. Additionally, the remote System administrator is advised to:

- use a long password - up to 49 characters can be used.
- use a mixture of upper and lower case letters, numbers and punctuation.
- change the password every month.

Note: *Log-on to Océ System Configuration is blocked for a while after an incorrect password is entered. The blocking interval is increased after successive incorrect entries.*

Security mode

By default, Océ delivers the DAC in the highest security mode: indicated by 'Security level: High (factory default)'. This provides the most restrictive set of operational settings.

Attention: The remote System administrator must not change the security mode. Otherwise the DAC is no longer in the certified configuration and is no longer able to assure the security of its objects and itself. It is not possible to get the DAC back into the certified configuration by changing the security mode back to 'High'.

E-shredding

By default, E-shredding is enabled for all data objects.

The following E-shredding settings can be configured:

- Number of overwrite passes (Default:'3 (U.S. DoD 5220.22-M)').
- Moment of overwriting (Default: 'Perform first pass at once, the rest in the background').

Attention: The remote System administrator must not change the 'Jobs to overwrite' settings. If E-shredding is disabled for 'scan jobs' or 'print jobs without security code', the DAC is no longer in the certified configuration and is no longer able to assure the security of 'scan jobs' and 'print jobs without security code'.

Log-on

Type the following link in the web browser to use the Océ System Configuration:

https://<hostname>/

Note: *To learn how to use the Océ System Configuration, refer to the On-line help of the Océ System Configuration (click the [?] button).*

Index