CryptoKey

Administration Guide

Trademarks

DualShield Unified Authentication, CryptoKey, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer

This document is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Northway House
1379 High Road
London N20 9LP
United Kingdom

Tel: +44(0)20 8343 9663
Fax: +44(0)20 8446 3182
Web: www.deepnetsecurity.com
Email: support@deepnetsecurity.com

Contents

Introduction

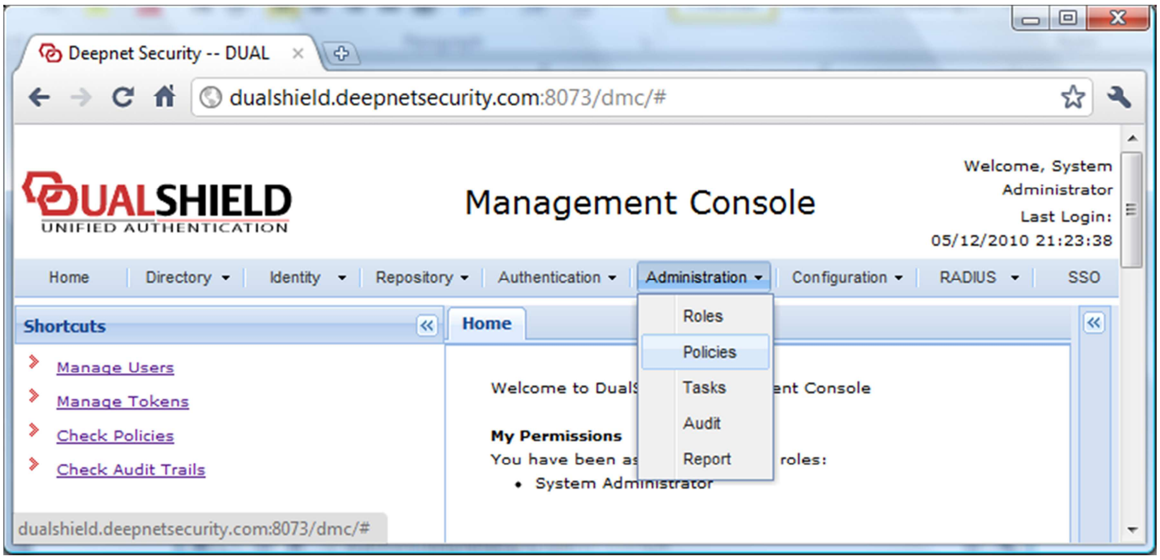
Deepnet CryptoKey drives can be centrally managed by IT administrators and help desk. The management facility of CrytoKey is built into the Deepnet DualShield Management Console which is a web-based management interface that manages user's accounts, identities, multi-factor authentication credentials and their authentication and encryption devices.

Registration

To minimise the administration work, CryptoKey is designed to enable end users to self-register their CryptoKey devices. Please see the CryptoKey User Guide for the information of the self-registration process.

The only thing that the administrator needs to set in the DualShield Management Console for the CryptoKey registration is the registration policy.

Select "Administration | Policies",

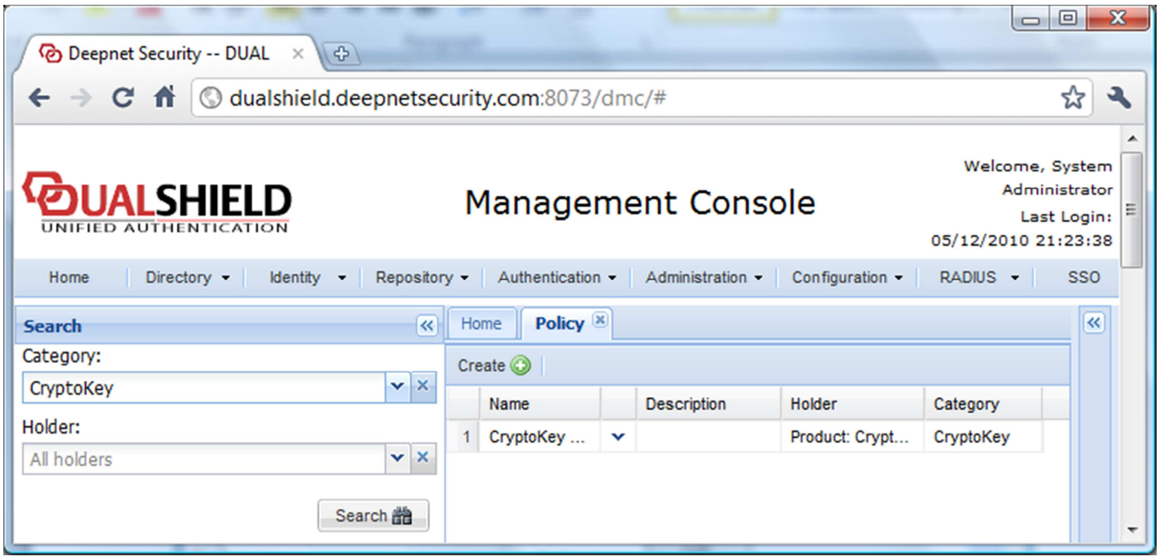


Welcome, System Administrator
Last Login: 05/12/2010 21:23:38

Welcome to Duals ent Console

My Permissions
You have been as roles:
- System Administrator

In the Search Panel on the left, select “CryptoKey” in the Category pull-down list,

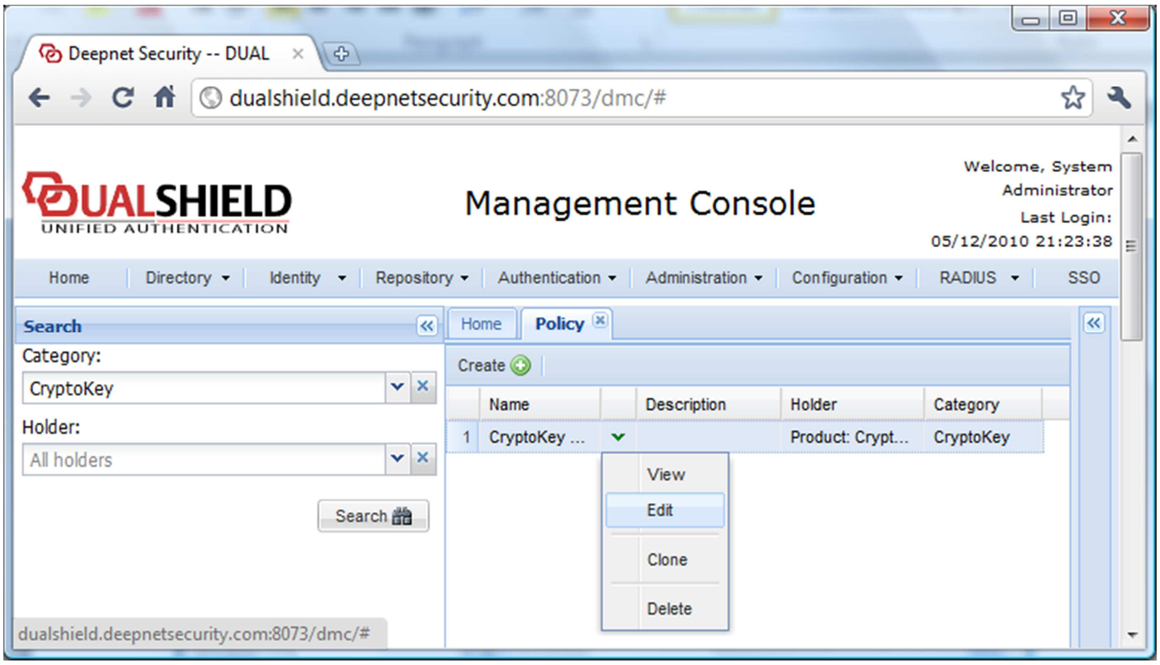


Category: CryptoKey

Holder: All holders

	Name		Description	Holder	Category
1	CryptoKey ...			Product: Crypt...	CryptoKey

In the Policy tab, click the CryptoKey’s context menu (down arrow) and select “Edit”

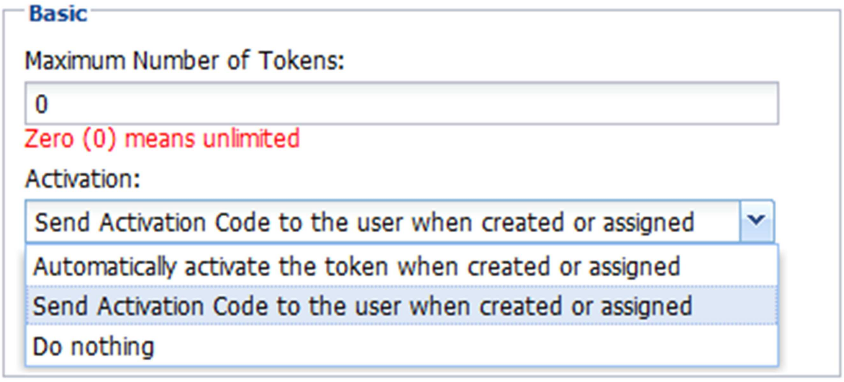


Category: CryptoKey

Holder: All holders

	Name		Description	Holder	Category
1	CryptoKey ...			Product: Crypt...	CryptoKey

The policy concerning the CryptoKey registration is “Activation”.


Basic
Automatically activate the token when created or assigned
Send Activation Code to the user when created or assigned
Do nothing

Maximum Number of Tokens: 0

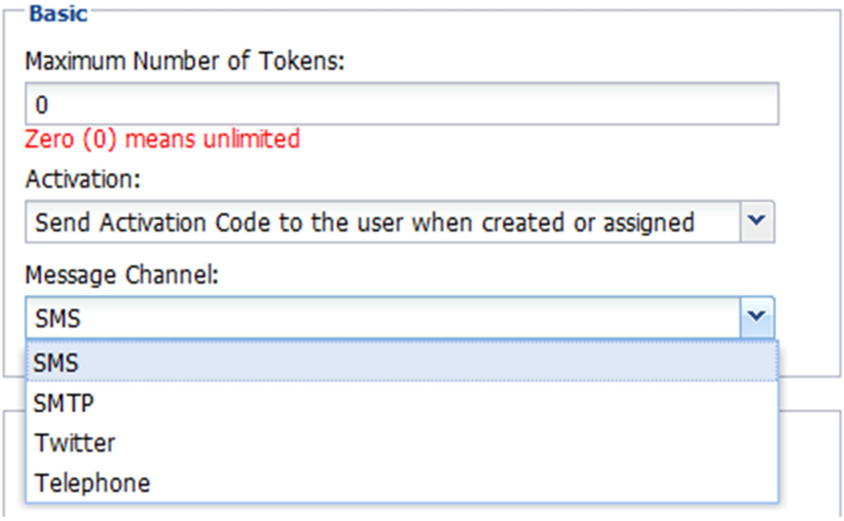
Zero (0) means unlimited

Activation: Send Activation Code to the user when created or assigned

If you wish to automatically activate CryptoKey registration select "Automatically activate the token when created or assigned"

If you want users to activate CryptoKey registration with an additional Activation Code, select "Send Activation Code to the user when created or assigned"

You can select how the Activation Code will be sent by selecting "Message Channels"



Basic

Maximum Number of Tokens: 0

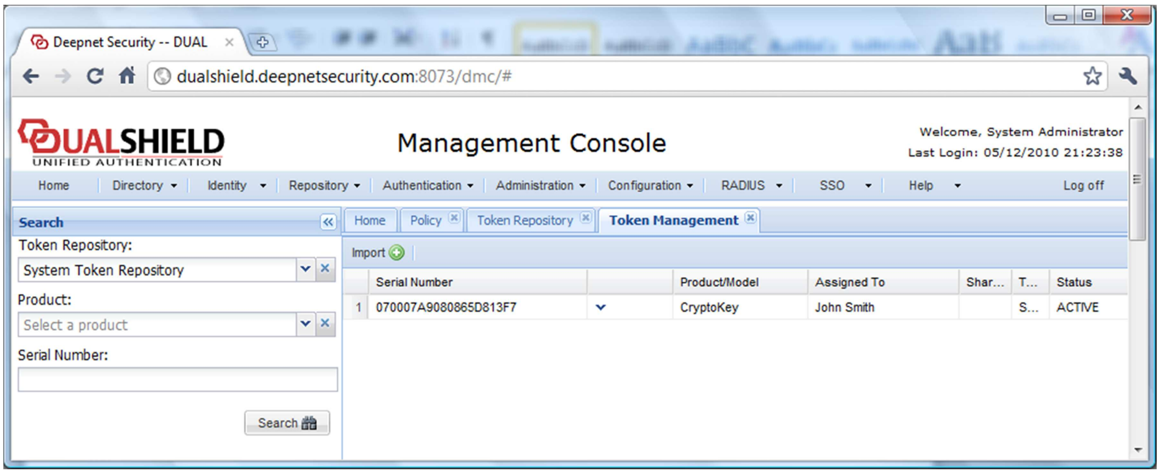
Zero (0) means unlimited

Activation: Send Activation Code to the user when created or assigned

Message Channel: SMS

Managing Devices

All registered CryptoKey devices are managed in the Token Repository.



Welcome, System Administrator

Last Login: 05/12/2010 21:23:38

Token Repository: System Token Repository

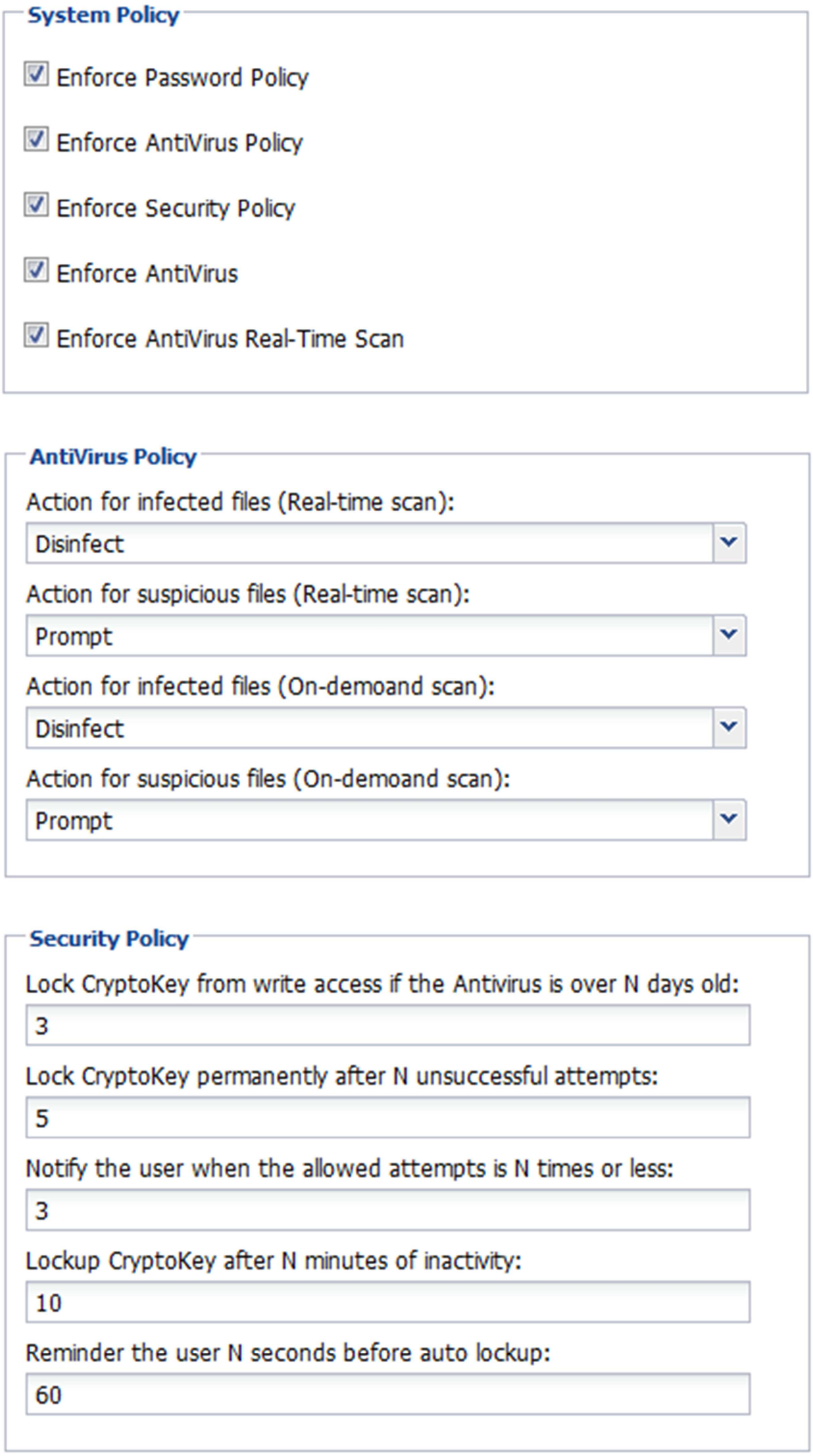
Product: Select a product

Serial Number:

	Serial Number		Product/Model	Assigned To	Shar...	T...	Status
1	070007A9080865D813F7		CryptoKey	John Smith		S...	ACTIVE

In the Token Repository, you can see a list of CryptoKey devices and their owners.

Managing Policies



System Policy

☑ Enforce Password Policy

☑ Enforce AntiVirus Policy

☑ Enforce Security Policy

☑ Enforce AntiVirus

☑ Enforce AntiVirus Real-Time Scan

AntiVirus Policy

Action for infected files (Real-time scan): Disinfect

Action for suspicious files (Real-time scan): Prompt

Action for infected files (On-demoand scan): Disinfect

Action for suspicious files (On-demoand scan): Prompt

Security Policy

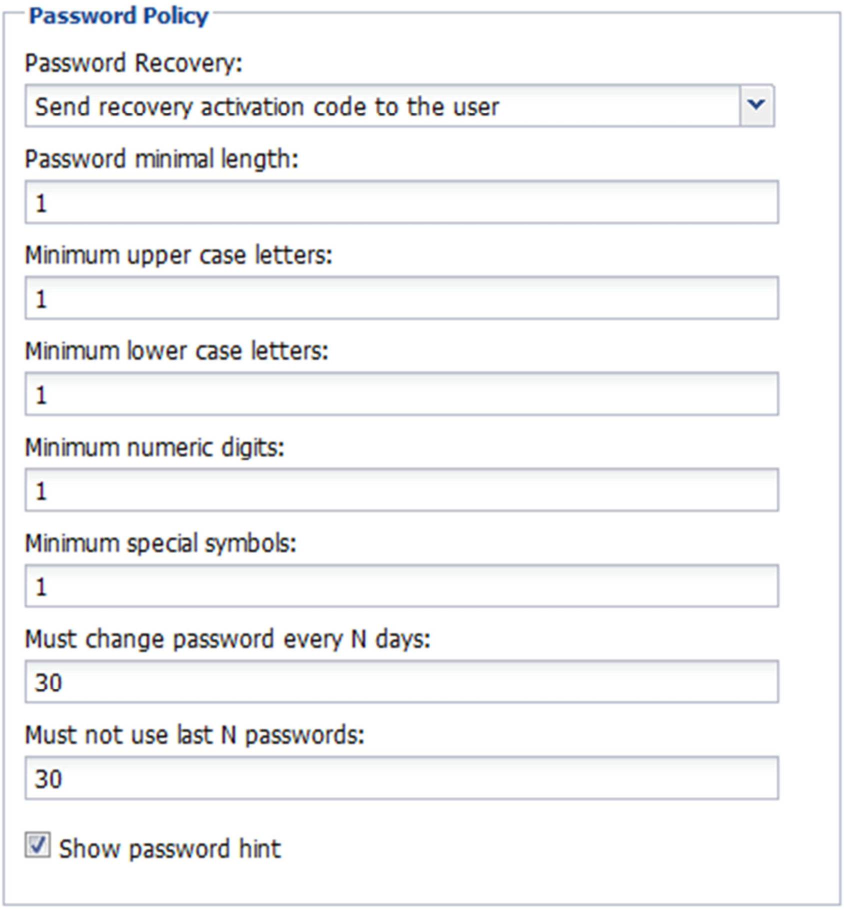
Lock CryptoKey from write access if the Antivirus is over N days old: 3

Lock CryptoKey permanently after N unsuccessful attempts: 5

Notify the user when the allowed attempts is N times or less: 3

Lockup CryptoKey after N minutes of inactivity: 10

Reminder the user N seconds before auto lockup: 60



Password Policy

Password Recovery:
Send recovery activation code to the user

Password minimal length:
1

Minimum upper case letters:
1

Minimum lower case letters:
1

Minimum numeric digits:
1

Minimum special symbols:
1

Must change password every N days:
30

Must not use last N passwords:
30

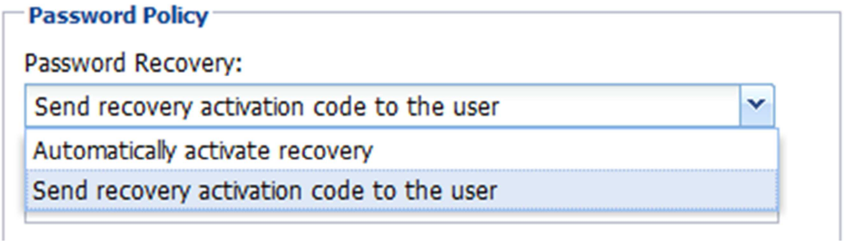
☑ Show password hint

Password Recovery

If a user has forgotten his/her password, he/she can recover the password in two ways, Automatic Recovery and Manual Recovery.

Automatic Recovery

In Automatic Recovery, the user will need to authenticate themselves by providing correct the username and password. The system administrator should set the Password Recovery and decide whether automatic recovery requires a further activation code.



Password Policy

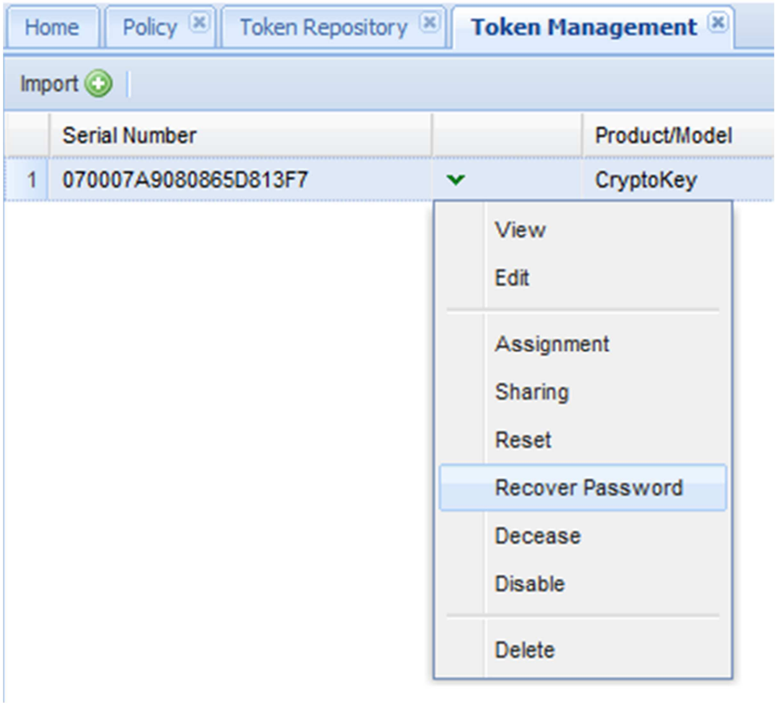
Password Recovery:
Send recovery activation code to the user

Automatically activate recovery
Send recovery activation code to the user

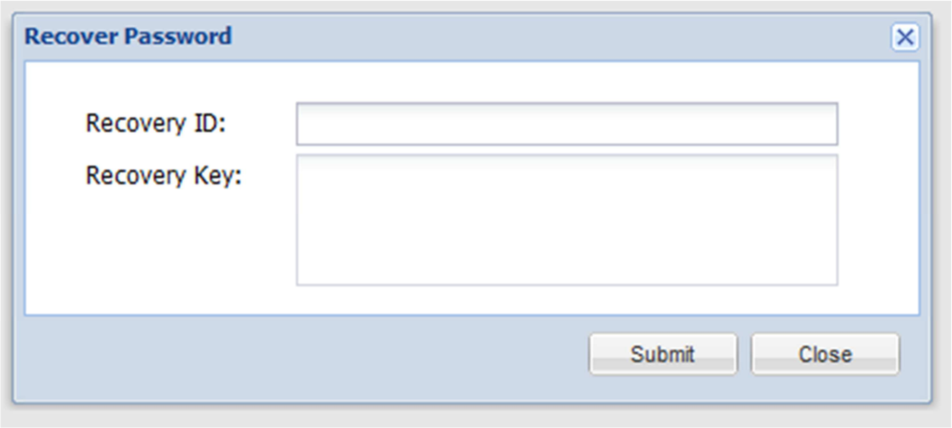
Manual Recovery

If a user choose to recover their password manually, then the user will contact the administrator or help desk and ask for a Recovery Code.

The user will provide the serial number of the device and a Recovery ID code. The administrator will locate the device in the token repository and select "Recover Password" from the context menu:

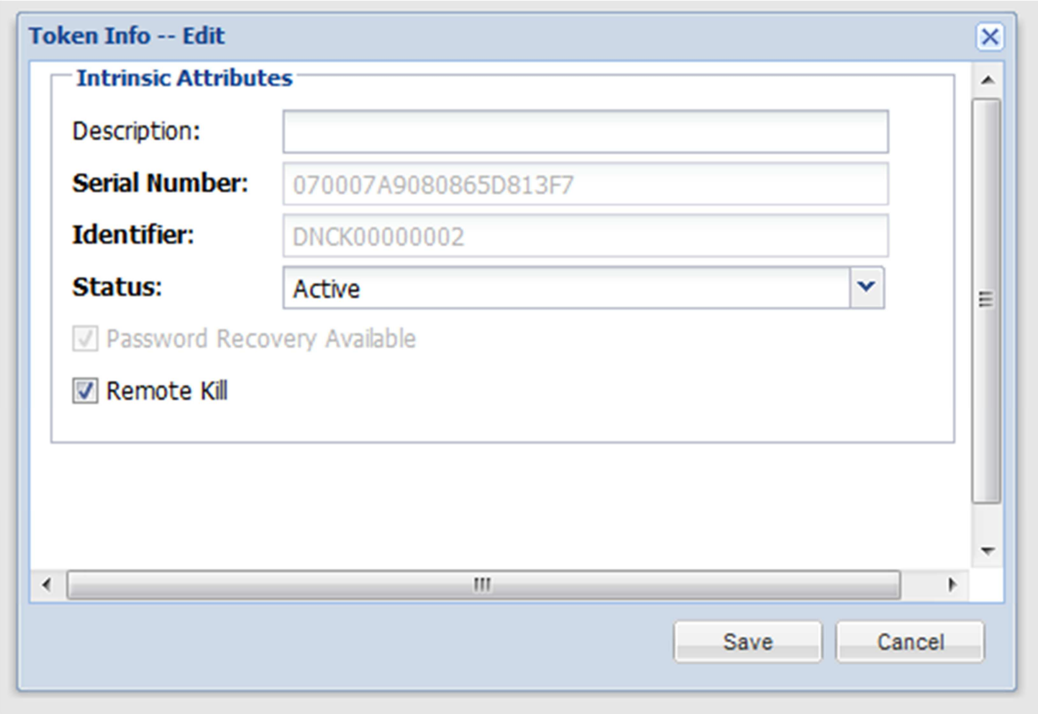


	Serial Number		Product/Model
1	070007A9080865D813F7		CryptoKey



Remote Kill

To remotely kill a CryptoKey device, locate the device in the token repository and select "Edit" from the context menu:



Token Info -- Edit

Intrinsic Attributes

Description:

Serial Number: 070007A9080865D813F7

Identifier: DNCK00000002

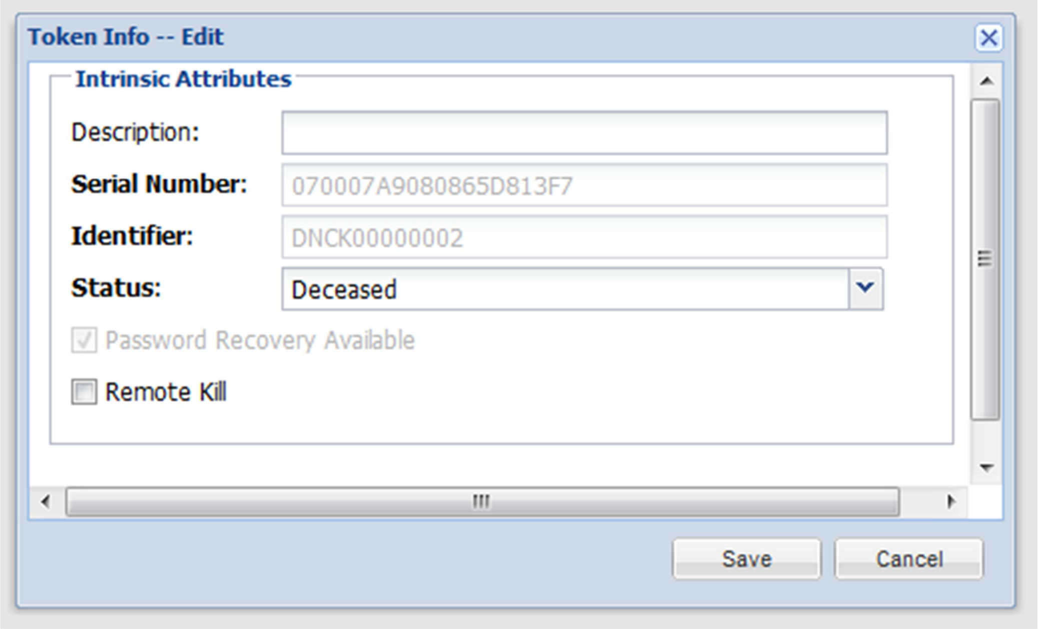
Status: Active

☑ Password Recovery Available

☑ Remote Kill

Then check (tick) the "Remote Kill" option.

If a CryptoKey device has been remotely killed, its status will show "deceased".



Token Info -- Edit

Intrinsic Attributes

Description:

Serial Number: 070007A9080865D813F7

Identifier: DNCK00000002

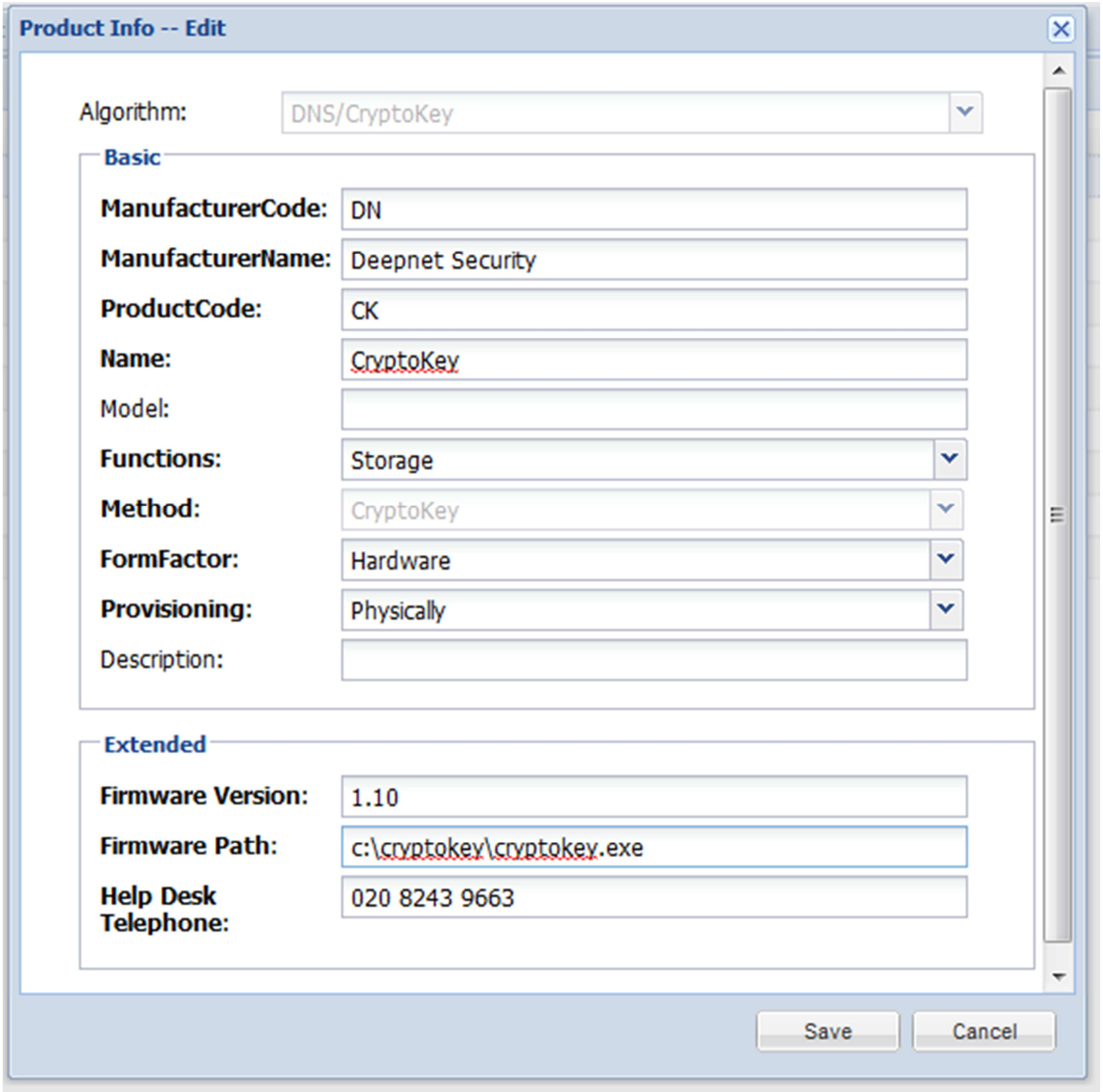
Status: Deceased

☑ Password Recovery Available

□ Remote Kill

Firmware Upgrade

When a new version of the CryptoKey's firmware is available, the administrator can inform users to upgrade their CryptoKey by simply entering the Firmware Version and Location in the CryptoKey's product properties.



Product Info -- Edit

Algorithm: DNS/CryptoKey

Basic

ManufacturerCode:	DN
ManufacturerName:	Deepnet Security
ProductCode:	CK
Name:	CryptoKey
Model:	
Functions:	Storage
Method:	CryptoKey
FormFactor:	Hardware
Provisioning:	Physically
Description:	

Extended

Firmware Version:	1.10
Firmware Path:	c:\cryptokey\cryptokey.exe
Help Desk Telephone:	020 8243 9663

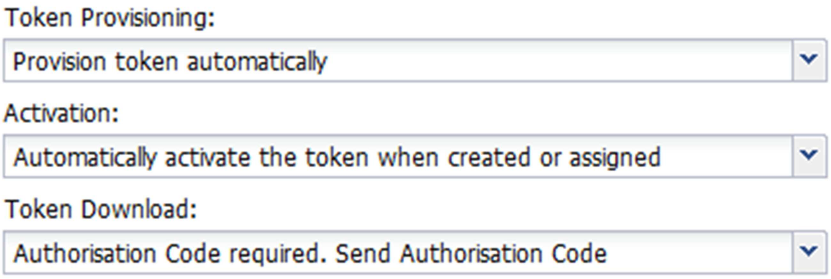
Two-Factor Authentication

CryptoKey can also be used as a two-factor authentication token. The Deepnet MobileID client is already built into the CrptoKey's console. To use MobileID, all the user needs is a MobileID token. Users can download their MobileID tokens from the management server automatically or they can install tokens manually with the help of the IT administrator or help desk.

Download MobileID Token

If you wish to enable your users to download their tokens automatically, there are two policy options you need to set in the MobileID's policy settings.

CryptoKey supports time-based MobileID token only. Select "MobileID/Time-Based" from the Policy Category list, then select "Edit" from its context menu.



Token Provisioning: Provision token automatically

Activation: Automatically activate the token when created or assigned

Token Download: Authorisation Code required. Send Authorisation Code

You should select "Provision token automatically" in the "Token Provisioning" option.

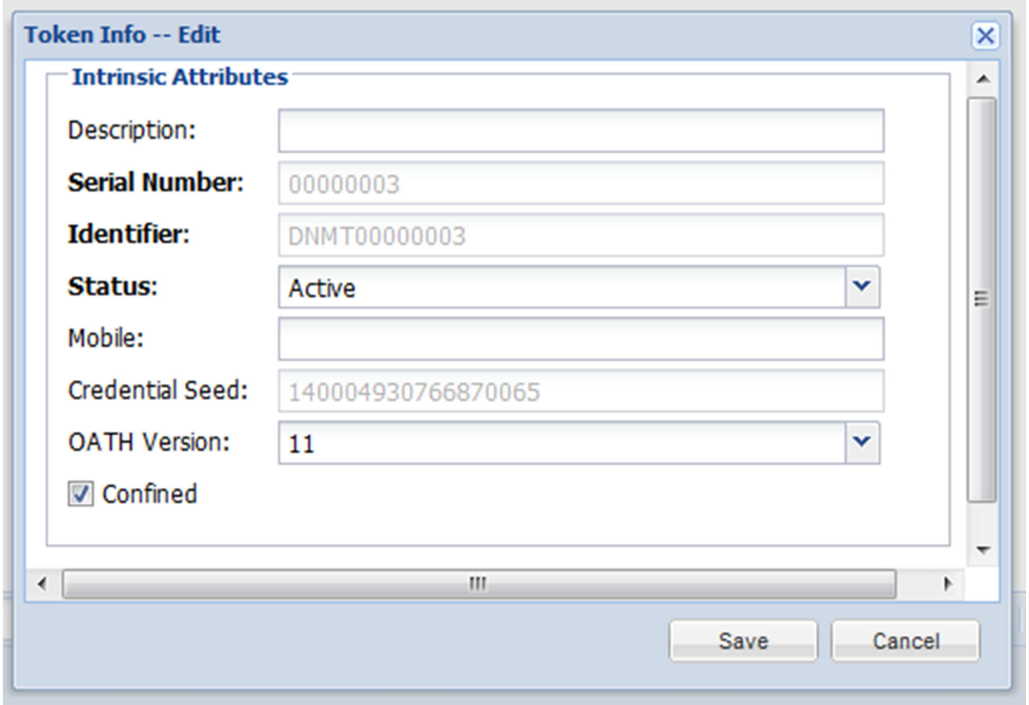
In the "Token Download" option, you have the following options:

- Authorisation Code not required
- Authorisation Code required. Send Authorisation Code
- Authorisation Code required. Do not Send Authorisation Code

If the Authorisation Code is not required then user will be able to download their tokens by providing their username and password only. Otherwise, users will be asked to provide an authorisation code as well.

Install MobileID Token

If you do not want your users to self-download their MobileID tokens, you will have to manually create a MobleID token in their accounts, then you will have provide them with the toekn’s serial number and seed data on request. These information can be obtained from the token’s properties:



Token Info -- Edit

Intrinsic Attributes

Description:

Serial Number: 00000003

Identifier: DNMT00000003

Status: Active

Mobile:

Credential Seed: 140004930766870065

OATH Version: 11

☑ Confined