

Trusted Client™

Mobile working environment provides secured remote access.

BeCrypt **Trusted Client** allows a user to **securely** access his or her organisation's network from any computer in any location.

Product summary

- Trusted Client is a bootable trusted environment that resides on a USB flash drive.
- Trusted Client devices are encrypted to ensure the integrity of the Operating System, and password-protected to prevent unauthorised access.
- When inserted into an unmanaged computer, Trusted Client launches a self-contained environment, entirely separate from its temporary host's operating system or hard drive, and leaves nothing behind when the session ends.
- The trusted environment typically provides a simple user interface, a web browser, and optional extra functionality, including thin-clients, email access, and stand-alone applications.
- When used with a third party VPN, such as Juniper or AEP, Trusted Client provides secure thin client functionality that may be used to remotely access enterprise applications.



- Configurable security features prevent accidental or deliberate misuse of the Trusted Client device by the authorised user.
- All data saved to a Trusted Client device is automatically encrypted.
- Trusted Client devices may optionally be managed via BeCrypt Protect Manager, providing an audit trail, and allowing the remote decommissioning of devices.

A revolutionary solution

Trusted Client is a bootable trusted environment that can be run on any unmanaged, untrusted platform. The Trusted Client environment, consisting of a lightweight Operating System, a web browser, and optional additional components (such as an SSL VPN, thin client applications, an email client), is written onto a USB flash drive. The USB device is protected by AES encryption and by strong user authentication, and may safely be carried by any authorised user.

Encryption & authentication

All sensitive data on the Trusted Client device, including the operating system, is protected by a **combination** of encryption and strong authentication. Only if the user enters the correct username and password will Trusted Client begin decryption and launch the trusted environment. If an unauthorised user tries to boot from the device, Trusted Client asks for a username and password; if the user inserts the device into a booted machine, Windows assumes that the device is unformatted (because it is encrypted) and prompts the user to format it. In neither case can the contents of the device be read, and they will be deleted if the user reformats.

Configurable security

Trusted Client's security features are configured according to an organisation's security policy by its system administrator. The configured setup file is then written to as many USB devices as required. Each Trusted Client device may have a unique encryption key, username and password and may be configured to require dual-factor authentication by Common Access Card. Restrictions may be set on the use of high-risk features to prevent accidental or deliberate misuse by the authorised user.



Restrictions include:

- **Allowed IP addresses.**
Trusted Client may be configured to connect only to allowed machines (IP addresses) and via specified ports.
- **Peripheral device access.**
Trusted Client may be configured to remove all possible data export paths from the device.
- **System Persistence.**
The environment is configured to prevent any unauthorised modifications to system files.
- **Password policy.**
Password format may be restricted to enforce **strong authentication**; alternatively, the user may be forced to use the embedded strong password generator.

CAC card support

Trusted Client devices may be configured to enforce dual-factor authentication using the authorised user's personal Common Access Card and PIN.

Clone protection

Trusted Client device automatically performs a self-test during bootup. If it fails the clone test, the device erases itself.

Wireless support

Trusted Client optionally connects to pre-defined remote servers using the host's connection and supports a range of wireless cards.

Remote management

When managed via BeCrypt Protect Manager, Trusted Client devices automatically contact the server on bootup (provided a connection can be established), and details may be viewed in the Protect Manager Console or the Windows Event Log. If the System Administrator has marked a device for revocation, Protect Manager replies with a decommission message, and the device immediately erases itself.

Device recovery

If the user forgets his or her device password, Challenge-Response provides a mechanism by which access may be regained with the aid of an administrator. Challenge-Response uses recovery data generated during installation. At no point in the Challenge-Response procedure is the user's original password exposed.

DISK Protect™

PC security solution combining full disk encryption with strong boot time authentication and optional removable media encryption. **DISK Protect 4.1** has been awarded the CSIA Claims Tested Mark; **DISK Protect Baseline** is CAPS-approved to Baseline; **DISK Protect Enhanced** is CAPS-approved to Enhanced grade.

Removable Media Module™

Cost effective encryption of data on removable storage devices such as USB Flash Drives, memory devices and SD Cards.

PDA Protect™

PDA security solution that enforces strong authentication, secured synchronisation and the encryption of removable memory cards. **PDA Protect 4.1** has been awarded the CSIA Claims Tested Mark; **PDA Protect Baseline** is CAPS-approved to Baseline.

Connect Protect™

Port Controller for desktop and laptop PCs manages access to Plug and Play devices. **Connect Protect 2.0** has been awarded the CCT Mark.

Trusted Client™

Secure, isolated, configurable operating system for use in an unmanaged environment providing functionality customised to an organisation's requirements. **Trusted Client 1.2** has been awarded the CCT Mark.

Protect Manager™

Centralised security management and auditing functionality for the enterprise.

© Copyright 2008
by BeCrypt Ltd.

All Rights Reserved.

The BeCrypt Logo and Trademarks
are owned by BeCrypt Ltd.

No material may be reproduced for any
purpose, private or commercial,
without prior written
permission from
BeCrypt Ltd.