Guidance

# End User Devices Security Guidance: Becrypt tVolution

Published

**Contents**



Becrypt tVolution is a locked down, customizable Linux operating system. It has been designed to provide a managed end user device solution for the enterprise. tVolution can be installed onto the hard drive of a laptop or desktop and is remotely managed via the Becrypt Enterprise Manager.

This guidance is applicable to a physical installation of the tVolution encrypted HDD OS supported by Becrypt Enterprise Manager. This guidance was developed following testing performed on a standard laptop device with a physical installation of a tVolution operating system, configured using the tVolution client version 5.1.1. Becrypt Enterprise Manager version 4.3.3 and 4.7.1 were used for the remote management of devices.

## 1. Usage scenario

Becrypt tVolution should be installed on laptops or desktops connecting remotely back to the enterprise over a VPN. This enables a variety of remote working approaches such as accessing OFFICIAL email; creating, editing, reviewing and commenting on OFFICIAL documents, and accessing the OFFICIAL intranet resources, the internet and other web-resources.

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the confidentiality and integrity of the traffic, and to allow the devices and data on them to be protected by enterprise protective monitoring solutions.
- Applications are limited on the tVolution platform and may only be installed by an administrator. The tVolution platform should be used as a thin client device to provide the user with a remote desktop environment.

## 2. Summary of platform security

This platform has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can best satisfy the security recommendations for more details about how each of the security recommendations is met.

| Recommendation | Rationale |
|---|---|
| 1. Assured data-in-transit protection | The Linux version of the Cisco AnyConnect VPN has not been independently assured to Foundation Grade. |
| 2. Assured data-at-rest protection | The data-at-rest encryption used by Becrypt tVolution has not been independently assured to Foundation Grade. |
| 3. Authentication | |
| 4. Secure boot | Secure boot is not supported on this platform. |
| 5. Platform integrity and application sandboxing | |
| 6. Application whitelisting | |
| 7. Malicious code detection and prevention | |
| 8. Security policy enforcement | |
| 9. External interface protection | |
| 10. Device update policy | Administrators must maintain awareness of patch sets released by Becrypt to ensure tVolution clients are kept up-to-date. |
| 11. Event collection for enterprise analysis | |
| 12. Incident response | |

## 2.1 Significant risks

The following significant risks have been identified:

- The Linux variant of the Cisco AnyConnect VPN is available, but has not been independently assured to Foundation Grade. Without assurance in the VPN there is a risk that data in transit could be compromised.
- The data-at-rest encryption has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance there is a risk that data stored on the device could be compromised.
- There is currently no secure boot mechanism on the tVolution platform. The integrity check feature used during configuration ensures integrity of the OS image during installation only.
- Critical patches are supplied by Becrypt and must be pushed to tVolution clients via an internal patch server. Additional non-critical patches or software updates are provided on a quarterly basis. This is the only method of applying patches and software updates. The administrator should maintain an awareness of software versions and the patch sets available, and ensure that applicable patches and software updates are requested in addition to those provided as standard.

# 3. How the platform can best satisfy the security recommendations

This section details the platform security mechanisms which best address each of the security recommendations.

## 3.1 Assured data-in-transit protection

Becrypt tVolution currently supports a selection of VPN clients, none of which are currently certified as assured IPsec software products under CESG's Commercial Product Assurance (CPA) scheme.

The Cisco AnyConnect VPN client has Windows and Apple OS X versions that are CPA certified. It supports mutual certificate-based authentication and can be configured to use CESG approved IPsec profiles, making it the preferred choice of VPN client.

## 3.2 Assured data-at-rest protection

The encrypted HDD variant of the Becrypt tVolution OS implements AES-256 encryption for data at rest. All non-null sectors of the disk within the data partitions are encrypted at rest. Keys are generated using a FIPS approved library and stored encrypted on the disk.

However, Becrypt tVolution does not implement full disk encryption and is unable to meet a number of mandatory requirements for assured software full-disk encryption products defined under CESG's CPA scheme.

Two features are available to reduce the risks associated with data-at-rest; these options can be configured during the Operating System setup stage:

- A non-persistent data option can be enabled to ensure that no user data is stored on the device.
- An auto shutdown option can be enabled with a shutdown time out to ensure that if left unattended for a period of time, the client is shut down and the data at rest encrypted.

## 3.3 Authentication

The tVolution OS uses Active Directory allowing the user to logon using their domain credentials. Credentials are entered at boot time prior to decryption. Successful authentication at this time enables decryption and implicitly authenticates the user to the device. If the screen is locked, credentials are required to gain access.

Keys are sent from the client to the Becrypt Enterprise Manager (BEM) on registration with the server. This allows the server to authenticate the client.

Domain credentials and a client certificate must be entered to establish the VPN. Additionally domain credentials are required to gain access to network resources such as Outlook Web Access and Remote Desktop.

Becrypt tVolution supports smart cards which can be used in addition to domain credentials.

## 3.4 Secure boot

There is currently no secure boot mechanism on the tVolution platform.

## 3.5 Platform integrity and application sandboxing

These requirements are met without any additional configuration.

An integrity check feature may be enabled which uses an RSA certificate to confirm that the OS image has not been modified prior to installation. However, this check only applies to the installer OS and the USB bootable OS.

## 3.6 Application whitelisting

These requirements are met without any additional configuration.

tVolution doesn't have an application whitelisting feature. However, the OS is configured with a single user who cannot modify the file system or install additional applications. Applications can only be installed during Operating System setup, or at a later time via the patch server.

## 3.7 Malicious code detection and prevention

The platform implicitly provides some protection against malicious code being able to run when configured as recommended. This is because it is not possible to install any applications and no data persists during a reboot.

Third party anti-malware products may be obtained for use with the cooperation of Becrypt. Content-based attacks can be filtered by scanning capabilities in the enterprise.

## 3.8 Security policy enforcement

The enforcement of security policies is enforced during Operating System setup, and some settings may be centrally managed via the Becrypt Enterprise Manager.

Settings applied during setup or centrally cannot be modified by the user.

## 3.9 External interface protection

These requirements are met without any additional configuration.

External interfaces are not made available to the user and the user cannot modify this access as no root or terminal access is available.

## 3.10 Device update policy

Security patches and device updates are managed by a central patch server and can be configured via the Enterprise Manager. The patching policy cannot be modified by the user. The patch server should be configured to not allow the user to defer updates.

Becrypt supply security critical patches, where relevant, within 30 days of the component owner making a patch available. Non-critical patches or software updates are made available within quarterly patch sets. The administrator should maintain awareness of software versioning and patching requirements and retrieve these patch sets promptly, to ensure the software running on the clients is up to date.

Patch sets should be uploaded to the patch server where they can be downloaded by clients. Patch sets should first be uploaded to the testing repository, which should be configured on a small number of test clients. After evaluation on the test clients, patch sets should then be uploaded to the live repository where they will be retrieved by live clients.

tVolution clients may be configured as thin clients, providing only the software required to make a secure RDP connection to a centrally managed device. This configuration, which minimizes the number of extensions, reduces the number of applications on the tVolution client which require patching.

### 3.11 Event collection for enterprise analysis

The Becrypt Enterprise Manager collects events and audits for all tVolution clients.

Event Log includes:

- OS Installations (success and failures)
- System Information reports from clients (all clients report to BEM on start-up)

Audit Log includes:

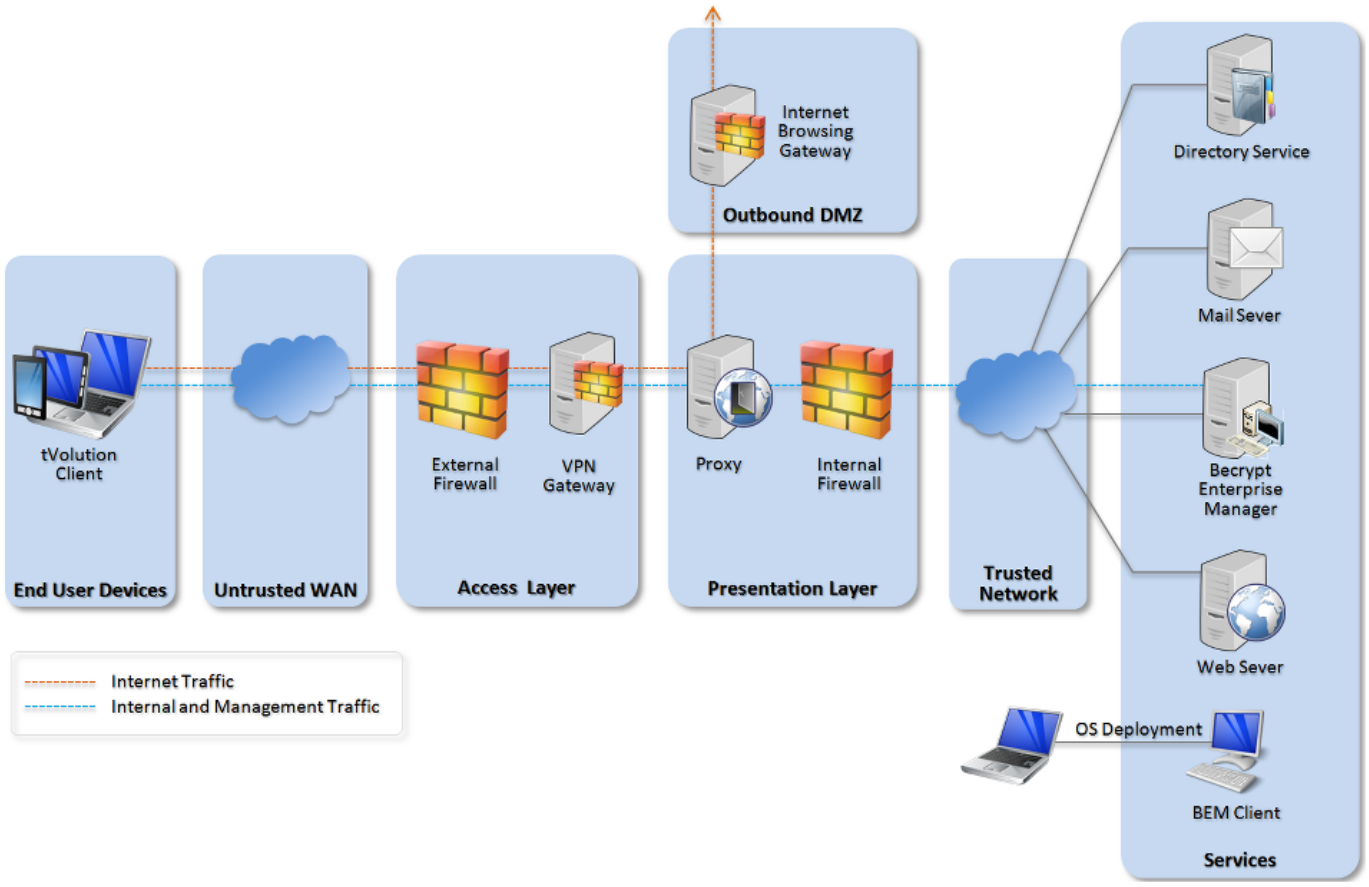
- User logins (success and failures)
- Client admin tasks, such as moving between policy groups
- Decommissioning logs

### 3.12 Incident response

tVolution clients may be remotely decommissioned via the Becrypt Enterprise Manager. However, remote decommissioning requires the client to connect to the server.

## 4. Network architecture

It is recommended that all remote or mobile working scenarios use a typical remote access architecture based on the Walled Garden Architectural Pattern.




**Recommended network architecture for deployments of Becrypt tVolution.**

## 4.1 Changes to facilitate tVolution

To facilitate tVolution, the following modifications are required:

### Internal firewall

The ports required for clients to reach the BEM server and patch server should be permitted on the internal firewall.

### Remote desktop architecture

A Terminal Server Gateway should be installed within the presentation layer to allow managed access to a Virtual Desktop Environment, if the tVolution client is to be used as a thin client.

# 5. Deployment process

For an enterprise deployment of tVolution that is suitable for organisations working with OFFICIAL data, administrators should carry out the following initial one time setup:

## 5.1 Environment setup

The following steps are required to deploy the Becrypt management components into the internal network:

1. Install and configure Becrypt Enterprise Manager Server and the tVolution Plugin
2. Install the Becrypt Enterprise Manager AD Plugin on the Active Directory server
3. Install and configure a Becrypt Patch Server with test and live patch repositories
4. Configure Active Directory and Group Policy as necessary
5. Install and configure the tVolution Setup Tool on a provisioning terminal

## 5.2 Customised operating system setup

Becrypt provide a base OS which has only basic drivers and software installed. The first stage of tVolution deployment is to use the tVolution Setup Tool to configure a base OS:

1. On the provisioning terminal, open the tVolution Setup Tool
2. Select the encrypted HDD base OS supplied by Becrypt (TC-HDD.tcs)
3. Step through the setup screens to configure the OS (recommended configuration options for the base OS are given in Main OS Setup)
4. Save the resulting OS with a chosen filename

## 5.3 Operating system installer setup

Once the base OS has been configured, there are two options for installing the OS onto devices. The first is remote installation over the network; the second is physical installation via a USB disk. Detailed instructions for both methods are available from Becrypt.

#### Remote installation

For remote installation via network share, the customised OS file must be stored on a network share and configured for deployment via Active Directory or SCCM.

#### Physical installation

For physical installation via USB, additional steps are required to configure a second installer OS and write all the required data to a USB device. Use the tVolution Setup tool to setup the tVolution installer OS as follows:

1. On the provisioning terminal, open the tVolution Setup Tool
2. Select the tVolution USB base OS (TC-USB.tcs)
3. Include the tcwriter tVolution extension
4. Select the customised OS created during the operating system setup as the installation file (multiple OS files may be selected)
5. Step through the rest of the setup, selecting the configuration options as described in Installer Setup
6. Save the resulting OS with a chosen filename.
7. Use the tVolution Writer tool to write the saved installer OS to a USB drive ready for provisioning
8. Step through the rest of the setup, selecting the configuration options as described in USB Writer Setup
9. Once the USB drive has been written it is ready to be used to install the OS onto the client

# 6. Provisioning steps

## 6.1 Device provisioning

The following steps should be followed to provision each device for distribution to end users. This assumes a physical installation has been chosen; for more information on the remote deployment options see the Becrypt tVolution documentation.

1. Boot from the installer USB disk, created during the operating system installer setup
2. Log in with the credentials set during the installer OS setup
3. Once booted, run the tVolution writer utility which will walk through installation of the main OS onto the target device
4. During device provisioning a temporary username and password must be chosen for the OS. The OS is synchronised with Active Directory, so a domain user must be selected

## 6.2 User provisioning

The following steps should be followed to customise each device for a given user. These steps require access to the domain and certificate infrastructure, and should therefore be carried out with the device connected to the internal network and the user present to enter

their credentials.

1. Boot the main OS, installed during device provisioning
2. Enter the temporary domain username and password set during device provisioning
3. When prompted, enter the end user's domain name and password to authenticate with Active Directory. At this point the tVolution credentials will synchronise to match the user's domain credentials.
4. Install the user's private key and certificate, as well as the certificate authority certificate for use in the VPN client
   - Certificates installed into the Firefox certificate store can be imported into Cisco AnyConnect using the Cisco Client Certificate Manager utility
5. Configure the system proxy to use the enterprise proxy for all traffic.

### 6.3 Notes

Once the OS is installed, it is not possible to make any administrative changes that require a terminal session or root privileges.

Policies are applied to groups within the Becrypt Enterprise Manager. All clients built using the encrypted HDD tVolution variant will automatically join the "Trusted Client" computer group in the Becrypt Enterprise Manager. An appropriate policy should be applied to this group to ensure that patches are applied to clients. A recommended policy is provided in BEM Policy Configuration.

## 7. Policy recommendations

This section details important security policy settings which are recommended for a Becrypt tVolution deployment. Other settings (e.g. server address) should be chosen according to the relevant network configuration.

### 7.1 Main OS setup

| Configuration Step | Recommended Setting |
|---|---|
| Setup file to configure | For a managed remote client, it is recommended that the TC-HDD.tcs base OS is selected as this provides encryption. |
| Optional system components | The base OS has limited drivers and software installed. At this point, the basic drivers and software should be selected and configured.<br><br>Recommended:<br>- Graphics driver<br>- Ethernet & Wi-Fi drivers |

| | |
|---|---|
| | - Remote desktop client<br>- Cisco AnyConnect VPN client<br><br>The number of extensions installed should be kept to a minimum, to reduce the attack surface. |
| Remote management | Select Becrypt Enterprise Manager to allow the client to be managed centrally by the server. |
| Authentication type | If used, select smart card authentication.<br><br>"Use an Active Directory or LDAP user account" is enabled by default. Password synchronisation should be enabled. |
| Security Options | Make Persistent: User data can be saved to the device: Disabled<br><br>Enable wireless connections: Enabled<br><br>Enable sound: Enabled<br><br>Enable video capture devices<br><br>Set shutdown dialog countdown Optional; set timeout as desired.<br>When disabled, the auto shutdown on idle will occur with no user warning, if enabled the user may persistently delay auto shutdown. If the client is configured as a thin client with no persistent data this should be disabled.<br><br>Enable screensaver: Enabled; set timeout as desired<br><br>Enable shutdown on idle: Enabled; set timeout as desired<br><br>Expiry Date: Optional<br>If enabled, the client will be decommissioned on the given date. Decommissioning causes the first sector of the disk to be wiped rendering the disk unbootable and encryption keys destroyed. |
| Restrict Allowed Hosts | Enabled<br><br>Remote host restriction allows the data in transit to be restricted to the VPN only. This enforces tunnel mode and prevents data in transit when the VPN is not established.<br><br>Allowed Hosts - Include:<br>- VPN Endpoint IP or domain<br>- Internal address ranges<br><br>Ensure all required ports are permitted including the proxy, BEM, patching and RDP. |
| Enable Patching | Enable<br><br>Configure for internal patch server; test clients should be configured to use the test server, all active clients should use the live patch server.<br><br>Enable customer-specific patch sets: Set as desired<br><br>Allow user to defer patching: Disable |

## 7.2 Installer OS setup (for physical installation)

| Configuration Step | Recommended Setting |
|---|---|
| Setup file to configure | For a managed USB installer, it is recommended that the TC-USB.tcs OS is selected as this provides encryption. |
| Optional system components | The installer OS has no drivers or software installed. At this point, the basic drivers and software should be selected and configured:<br>- Graphics driver<br>- Ethernet & Wi-Fi drivers<br><br>Additionally, the tcwriter extension is required to write the main tVolution OS to a hard drive |
| Load a tVolution Setup File | The tVolution setup file for the main OS (created previously) should be selected at this point. Multiple TCS files may be included. |
| Remote Management | Select Becrypt Enterprise Manager to allow the client to be managed centrally by the server.<br><br>Although the installer OS will not require ongoing central management, it will allow for remote decommissioning in the event that the USB is lost or stolen, and provides logging of use. |
| Installation Type | Optional: chosen by the administrator |
| Authentication Type | Password only authentication.<br><br>"Use an Active Directory or LDAP user account" is enabled by default. Password synchronisation should be enabled. |
| Security Options | Make Persistent: User data can be saved to the device: Disabled<br><br>Enable wireless connections: Enabled<br><br>Enable sound: Enabled<br><br>Enable video capture devices<br><br>Set shutdown dialog countdown Optional; set timeout as desired.<br>When disabled, the auto shutdown on idle will occur with no user warning, if enabled the user may persistently delay auto shutdown. If the client is configured as a thin client with no persistent data this should be disabled.<br><br>Enable screensaver: Enabled; set timeout as desired<br><br>Enable shutdown on idle: Enabled; set timeout as desired<br><br>Expiry Date: Optional<br>If enabled, the client will be decommissioned on the given date. Decommissioning causes the first sector of the disk to be wiped rendering the disk unbootable and encryption keys destroyed. |
| Enable Integrity Checking | Enable<br><br>Configure with an appropriate signing certificate to ensure integrity of the installation media during client installation. |

| | |
|---|---|
| Enable Patching | Enable<br><br>Configure for internal patch server; test clients should be configured to use the test server, all active clients should use the live patch server.<br><br>Enable customer-specific patch sets: Set as desired<br><br>Allow user to defer patching: Disable |

## 7.3 USB writer setup

| Configuration Step | Recommended Setting |
|---|---|
| Open TCS File | Select the configured Installer OS |
| Configure User Credentials | These are the credentials to be used by the administrator performing the installation. A temporary password may be given at this time as the USB installer client will synchronise with Active Directory on first boot. |
| Integrity Checking | If integrity checking of the installation OS was enabled, you are required to enter the certificate passphrase here to sign the device. |
| Expiry Date | Optional<br><br>This applies to the installer USB OS only. If enabled, the installer USB will be decommissioned on the given date. Decommissioning causes the first sector of the drive to be wiped rendering the disk unbootable and encryption keys destroyed. |
| Select Removable Drive | Select a removable drive for installation of the installer OS. Ensure that a blank drive is used as all data will be wiped. |

## 7.4 BEM policy configuration

| Configuration Step | Recommended Setting |
|---|---|
| Patch Policy | Active<br><br>Configure with appropriate patch server settings<br><br>Disallow users to defer patching<br><br>This policy should be set in addition to the settings applied during OS configuration. |
| Client Security Policy | Active<br><br>Currently, the only setting configurable by policy is the Device Shutdown on idle timeout. This |

## 7.5 VPN Configuration

The Cisco AnyConnect VPN client supports the VPN configurations outline in CESG's Commercial Product Assurance (CPA) scheme. The AnyConnect client will establish a connection based on parameters defined on the VPN endpoint.

The endpoint should be configured to use either of the following IPsec profiles:

Interim Profile (until 2015):

- Key Exchange: IKEv1
- Encryption: AES-128 in CBC mode
- Pseudo-random function: SHA-1
- Diffie-Hellman group: Group 5 (1536 bits)
- Signature: RSA with SHA-1 with X.509 certificates

End-State Profile:

- Key Exchange: IKEv2
- Encryption: AES-128 in GCM-128
- Pseudo-random function: HMAC-SHA256-128
- Diffie-Hellman group: Group 19
- Signature: ECDSA-256 with SHA256 on P-256 curve with X.509 certificates

# 8. Enterprise considerations

The following points are in addition to the common enterprise considerations, and contain issues specific to deployments of Becrypt tVolution devices.

## 8.1 tVolution OS Variations

tVolution is a configurable OS. A number of base OS files are provided by Becrypt, these can then be configured using the tVolution setup tool. The existing OS variations are listed below.

| Filename | Description | Encryption | Integrity Check | Runs From |
|---|---|---|---|---|
| Tvolution.tcs | Base OS: unencrypted | None | None | HDD |

| | | | | |
|---|---|---|---|---|
| TC-USB.tcs | Base OS: USB bootable | AES-256 | Optional | USB Drive |
| TC-HDD.tcs | Base OS: encrypted | AES-256 | None | HDD |

### 8.2 tVolution Installation

Once a base OS has been chosen, Becrypt provide instructions for two installation methods; physical and remote. Physical installation uses a USB bootable installer and remote installation (also called zero-touch installation) requires third party package management software such as Active Directory or SCCM.

The installation mechanism does not affect the features of the OS, as the same OS may be installed via either installation mechanism.

## Legal information