deviceTRUST

Contextualizing IT *Simple. Dynamic. Integrated.*

Product Data Sheet

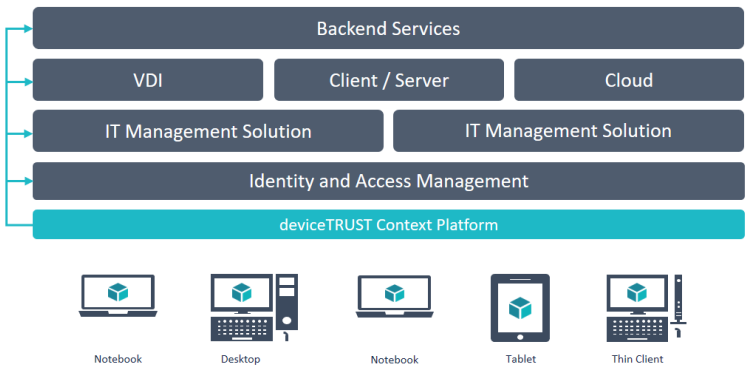
deviceTRUST´s mission is to contextualize the corporate enterprise, allowing users the freedom to access their corporate workspace from any location, on any device, over any network, while giving IT departments the information and control they need to meet their governance requirements.

With its patent pending technologies, deviceTRUST delivers more than 200 hardware, software, network, security, performance and location contextual properties into the virtual and physical workspaces. deviceTRUST can easily integrate with any existing workspace management solution and requires no additional infrastructure. The context is always up-to-date and any change triggers a definable action.

deviceTRUST - Contextualizing IT

Benefits

- **Meet Security, Compliance and Regulatory requirements by incorporating the endpoint and user context into business policies**
- **One central context platform – Rich set of detailed context**
- **Seamless integration into existing management and reporting solutions**
- **No additional infrastructure required - Easy and fast implementation**
- **Subscription based licensing**
- **Immediate Return on Investment (ROI)**



deviceTRUST

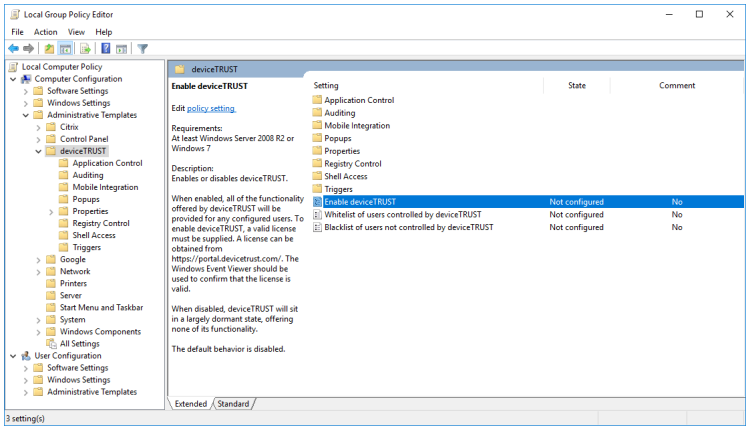
Phone: +49 (6162) 8015950
Email: info@devicetrust.com
https://devicetrust.com
Twitter: @deviceTRUST

CITRIX Ready fslogix Microsoft BizSpark Startup

deviceTRUST

Contextualizing IT *Simple. Dynamic. Integrated.*

Simple



deviceTRUST makes the context of the endpoint and the user available inside the virtual session and on the endpoint. The intelligent technology provides the context in a way that makes it easy consumable. It enables seamless support for internal and external network access, integrates transparently with existing VPN solutions and requires no additional infrastructure making implementation easy.

Dynamic

deviceTRUST ensures that all changes to the endpoint and user context results in an immediate update to the context within the virtual session and on the endpoint. Dynamic triggers allow the desktop to react to these changes. For maximum flexibility, these triggers can execute any script or process in the context of the logged on user or with system privileges.

Integrated

The context of the user and endpoint is written to the Microsoft Event Log, allowing easy integration with existing SIEM and reporting solutions.

Features

No infrastructure: deviceTRUST does not require any additional infrastructure. This enables a rapid and effective implementation and results in low implementation and operational costs.

Intuitive management: The configuration within Microsoft Active Directory GPO enables easy implementation and management of deviceTRUST.

Easy start: Group memberships allow you to easily target the users enabled for deviceTRUST functionality.

Seamless integration: The intelligent technology provides the context of the endpoint into the virtual session and on the endpoint, enabling easy consumption by all existing management solutions.

Always up-to-date: The context of an endpoint is kept up-to-date during the entire user session. This guarantees that all security and compliance requirements are met even if the status of the endpoint changes.

Endpoint support: All properties that represent the context of the endpoint are also available on the endpoint and can easily be used e.g. by access gateways as well as locally on the endpoint.

User messages: Depending on the context of the endpoint, user-dependent notifications can be displayed to the user.

Multilanguage support: All of the user messages available within the deviceTRUST Configuration can be translated.

Conditional Access: Control access to the virtual session depending upon whether a deviceTRUST client is installed and defined properties of the endpoint, independently from how the virtual session is accessed (internal / external network access). If the endpoint does not meet your requirements, the virtual session can be blocked for the user during logon and during the entire session.

Available properties: deviceTRUST policy settings can be used to define which properties of the endpoint are to be provided by deviceTRUST. Properties you do not need are not determined by deviceTRUST and thus are not available on the endpoint or within the virtual session. In addition, it is possible to define to which changes in the properties of the endpoint the triggers should react.

Easy deployment: All deviceTRUST components can be installed with existing software deployment solutions. The client can be installed for all users or per user.

deviceTRUST

Contextualizing IT *Simple. Dynamic. Integrated.*

Detailed information: deviceTRUST delivers more than 400 hardware, software, network, security, performance, printer and location properties into the virtual session and over 200 properties on the endpoint.

Geolocation: deviceTRUST makes it possible to provide the location of an endpoint regardless of the network connection used. This allows regulatory requirements with regard to site-based application access to be adhered to.

Note: *Geolocation requires integration with a GEO location provider, and may be subject to third party terms and conditions.*

Detailed security information: deviceTRUST provides a rich set of detailed information about the security state of the endpoint. The status of the Windows Update, Windows Defender and Windows Firewall can be consumed to control access to the virtual session or grant or deny access to applications.

Trigger: Respond to events within the users' session with triggers for Logon, Logoff, Disconnect, Reconnect, Desktop Starting, Desktop Ready and Property Change with user- or system privileges.

Microsoft® AppLocker Support: Based on the context of the user and the endpoint deviceTRUST can dynamically configure Microsoft® AppLocker to grant or deny access to applications, e.g. to meet license compliance requirements.

Application termination: If the context of the user and the endpoint does not meet the requirements anymore, deviceTRUST is able to terminate running applications.

Double-hop support: All context information of the user and the endpoint are available within all sessions of the user (Multi-hop).

Reporting: Detailed information, including the context of the endpoint and the user is reported by seamlessly integrating with existing reporting solutions. This gives new insight into the context of your virtual sessions and your endpoints. It is possible to define granularly which properties of an endpoint are not included in the reporting.

Attractive license model: deviceTRUST is licensed on a named-user basis independent how many endpoints a user is using. The subscription model prevents high investments.

Auto Update Client: The deviceTRUST Client can be downloaded by the user via a download link. New versions of the client can be installed automatically and without user intervention.

Secure communication: In addition to encryption using the underlying remoting protocol, all communication is encrypted using a 2048-bit RSA key and a 256-bit AES GCM stream cipher.

Requirements

Supported Windows Operating System (32-bit & 64-bit):

- Microsoft Windows 7
- Microsoft Windows 8.x
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Supported Mobile Operating System:

- Apple iOS 8.x / 9.x / 10.x / 11.x

Supported IGEL Operating System:

- IGEL OS 10.3.500 or higher

Supported Remoting Technologies:

- Microsoft Remote Desktop Protocol (RDP)
- Citrix Independent Computing Architecture (ICA)
- Amazon WorkSpaces PC-over-IP (PCoIP)