deviceTRUST

# Context awareness with IGEL & deviceTRUST

Simple. Dynamic. Integrated.

## Joint Solution

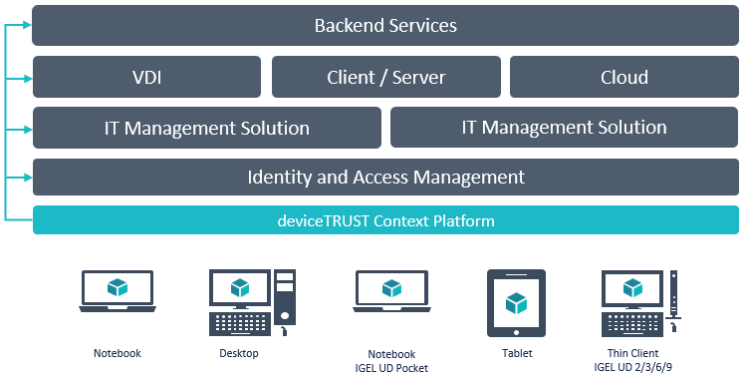
Modern workspaces imply major challenges for IT departments. Users work in a wide variety of locations, in diverse networks and with a wide variety of devices. Nevertheless, all safety, compliance and regulatory requirements must be met. deviceTRUST offers a comprehensive solution for this.

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.

The deviceTRUST client is pre-installed in IGEL's own Linux-based operating system IGEL OS (version 10.03.500 or higher) and can be easily activated via the IGEL Universal Management Suite (UMS).

### 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 of Investment (ROI)




CITRIX Ready


**deviceTRUST**

Email: info@devicetrust.com
https://devicetrust.com
Twitter: @deviceTRUST

**IGEL**

Email: info@igel.com
https://www.igel.com
Twitter: @IGEL_Technology

# deviceTRUST

## Simple

deviceTRUST makes the context of the IGEL endpoint and the user available within a virtual channel for Citrix and RDP sessions. 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 IGEL endpoint and user context results in an immediate update to the context within the virtual session. 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 IGEL 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. The deviceTRUST client is already implemented in the IGEL OS. 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, 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.

**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.

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

**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.

**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.*

**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.

**Supported IGEL endpoints:** By integrating the deviceTRUST client into the IGEL OS 10 firmware, its functionality is available on all IGEL Universal Desktop Thin Clients, IDEL UD Pocket, IGEL Zero Clients and on devices converted with the IGEL Universal Desktop Converter.

## About IGEL

IGEL delivers powerful unified endpoint management software that is revolutionary in its simplicity and purpose-built for the enterprise. The company's world-leading software products include the IGEL OS™, Universal Desktop Converter™ (UDC), IGEL Cloud Gateway™ (ICG), IGEL UD Pocket™ (UDP) and Universal Management Suite™ (UMS). These solutions enable a more secure, manageable and cost-effective endpoint management platform across nearly any x86 device. Additionally, IGEL's German engineered and manufactured thin, zero and all-in-one client solutions deliver the industry's best warranty (5 years), support (3 years after end of life) and management functionality. IGEL enables enterprises to precisely control all devices running IGEL OS as well as Windows OS from a single dashboard interface. IGEL has offices worldwide and is represented by partners in over 50 countries.