

## FSLogix Masking & deviceTRUST Contextual Access

Simple. Dynamic. Integrated.

### Joint Solution

FSLogix uses a unique approach, called Image Masking. This allows applications to be installed into any Windows environment, physical or virtual, exactly as intended by the software vendor, using the standard MSI or installation tools. With a superset of applications installed on one gold image, all users get the same image and the FSLogix solution simply hides all the applications they are not allowed to use.

deviceTRUST makes the context, of the endpoint and the user, available inside the virtual session and on the endpoint, to ensure that all changes to the endpoint and user context results in an immediate update.

deviceTRUST triggers FSLogix to make the application either accessible or inaccessible within the users' session. This strong combination of FSLogix Image Masking and deviceTRUST is the first solution that enables true contextual application access control for virtual and physical environments.

#### Business values:

- Reduce the number of gold images for all access scenarios
- Reduce license, support and management costs
- Secure and license-compliant application access

**Compliant device based licensing** Identify the endpoint within the virtual session based on the devices serial number to grant access to device based licensed applications only from licensed devices.

**Location based access** Grant or deny access to applications based on the geolocation of the endpoint to fulfill regulatory requirements.

**Endpoint security state** Critical applications and their data are only accessible if the security state (anti-virus, firewall etc.) of the endpoint meets the existing security and compliance requirements.

**Corporate / non-corporate devices** Grant access to specific applications only for corporate owned devices based on the domain membership of the endpoint.

#### deviceTRUST

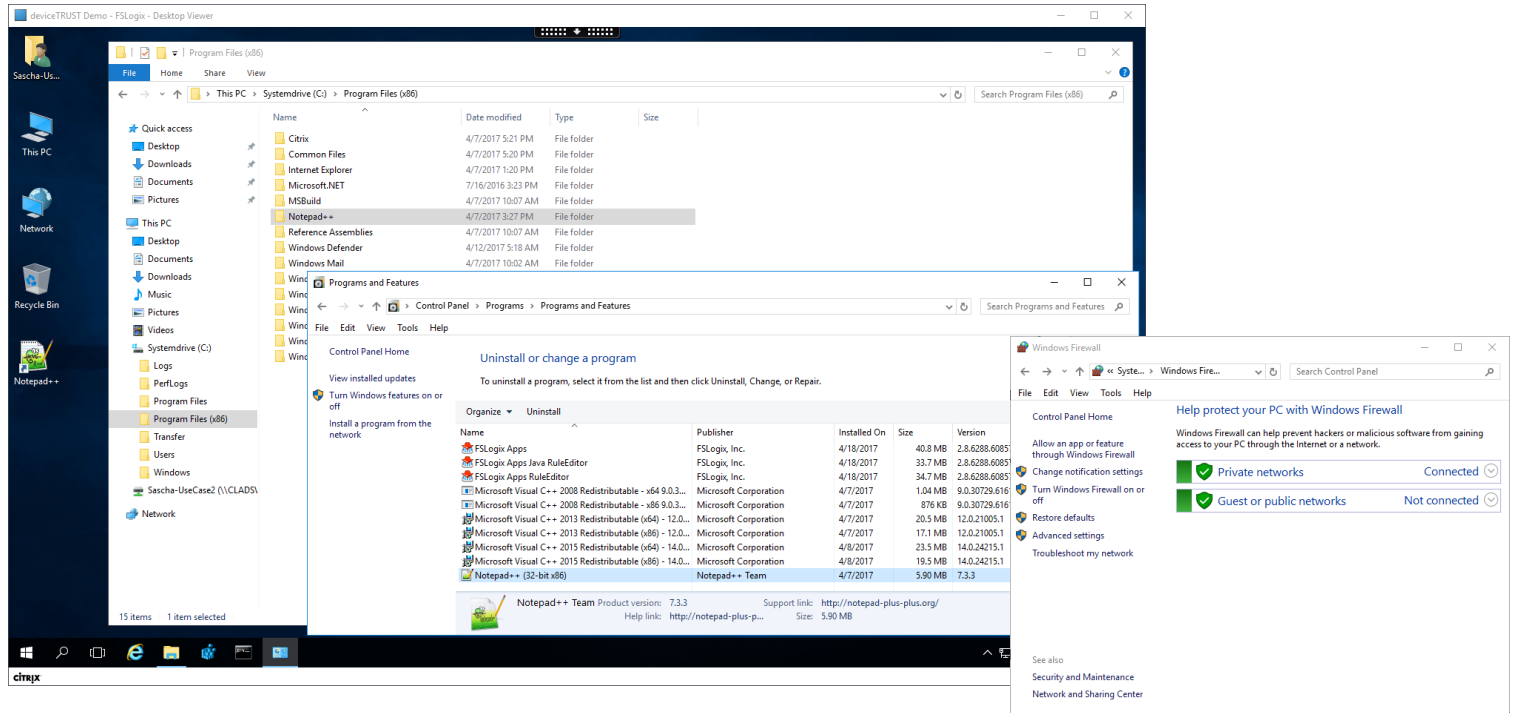
Email: [info@devicetrust.de](mailto:info@devicetrust.de)  
<https://devicetrust.com>  
Twitter: @deviceTRUST

#### FSLogix

Email: [sales@fslogix.com](mailto:sales@fslogix.com)  
<http://fslogix.com>  
Twitter: @fslogix

## Example: Application masking dependent on the security state of the endpoint

The endpoint security state does meet the required state and therefore the application **Notepad++** is visible and accessible within the users' session:



The endpoint security state does not meet the required state and therefore the application **Notepad++** is not visible and not accessible within the users' session:

