

# Home Office

19.4.100

*“For the successful implementation of a home office concept, it is essential that the employees receive almost the same working environment as in the company. In order to meet the existing security and compliance requirements as well as all regulatory requirements, it is necessary to ensure that employees actually work from their authorized home office.”*

## Step 1: Compliance Check

- deviceTRUST Client availability
- Access Mode
- Authorized Country
- Secure Network (No unsecure WiFi network)
- User Privileges
- Device Access (No remote-controlled device)
- Corporate Device
- Secure Device
- ...

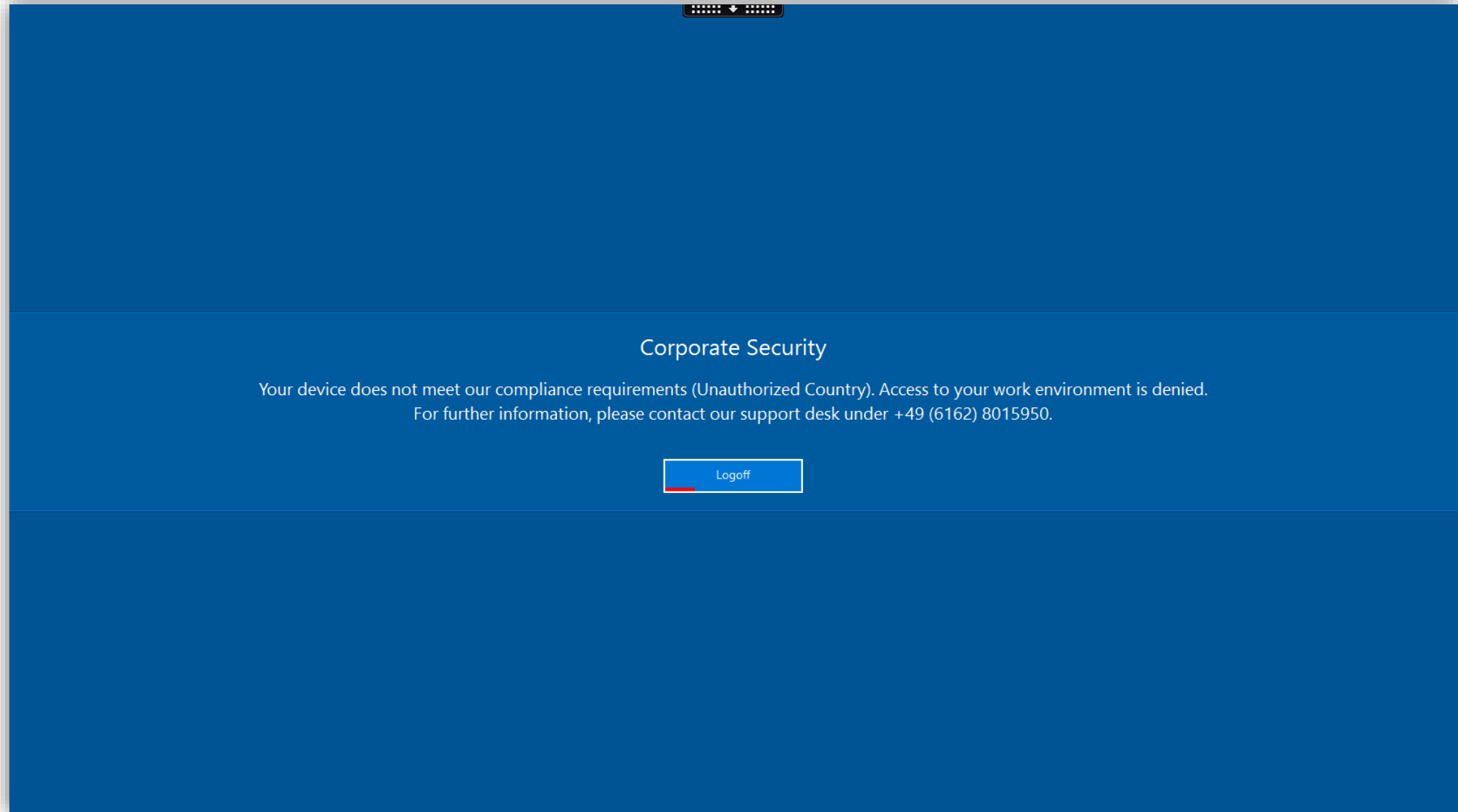
# Step 1: Compliance Check



The screenshot displays the 'Context' management page in the deviceTRUST application. The page includes a navigation bar with 'Home', 'Context', 'Actions', 'Messages', and 'Settings'. Below the navigation, there is a 'Context' section with an explanatory paragraph: 'Create the contexts that are important to your business. Each context is evaluated using properties from the remote device or the local host. They are assigned a value which can be acted upon by a task.' A search filter is present above a list of contexts. A dashed box highlights the 'Create new context' button. The list of contexts includes: Access Mode, Country, Detected Home Office, deviceTRUST Client, Remote Controlled, Security State, Validated Home Office, and WiFi Secure. Each context entry has a description and a toggle switch.

Context Name	Description	Toggle	Delete
<b>Create new context</b>			
<b>Access Mode</b>	Determines whether the remote device is internal or external to the corporate network.	On	Yes
<b>Country</b>	Determines the country in which the remote device is located.	On	Yes
<b>Detected Home Office</b>	Determines the detected home office of the user.	On	Yes
<b>deviceTRUST Client</b>	Determines the availability of the deviceTRUST Client on the remote device.	On	Yes
<b>Remote Controlled</b>	Determines whether the remote device is remote controlled.	On	Yes
<b>Security State</b>	Determines the security status of the remote device.	On	Yes
<b>Validated Home Office</b>	Determines the validated home office of the user.	On	Yes
<b>WiFi Secure</b>		On	Yes

# Step 1: Compliance Check



## Step 2: Validate and Detect

- Validate the current home office environment
- Detect current environment and make sure it is the home office

# Step 2: Validate and Detect



The screenshot shows the 'Actions' page in the deviceTRUST interface. At the top, there is a navigation bar with the 'deviceTRUST' logo and menu items: Home, Context, Actions, Messages, and Settings. On the right side of the navigation bar are icons for save, share, delete, and help. Below the navigation bar, the page title 'Actions' is displayed, followed by a descriptive paragraph: 'Actions can be used to execute a sequence of tasks on either changes to context or on predefined triggers during the lifetime of a user session.' A search bar with a magnifying glass icon and the placeholder text 'Filter' is located below the paragraph. A dashed-line box highlights a button with a plus sign and the text 'Create new action'. Below this, there are two sections of actions. The first section is labeled 'Very High' and contains one action: 'Home Office Conditional Access - Compliance Check' with a sub-description 'Applies conditional shell access policies for home office users.' and a toggle switch and delete icon. The second section is labeled 'High' and contains one action: 'Home Office Conditional Access - Validate and Detect' with a sub-description 'Applies conditional shell access policies for home office users.' and a toggle switch and delete icon.

deviceTRUST Home Context Actions Messages Settings

## Actions

Actions can be used to execute a sequence of tasks on either changes to context or on predefined triggers during the lifetime of a user session.

Filter

**+ Create new action**

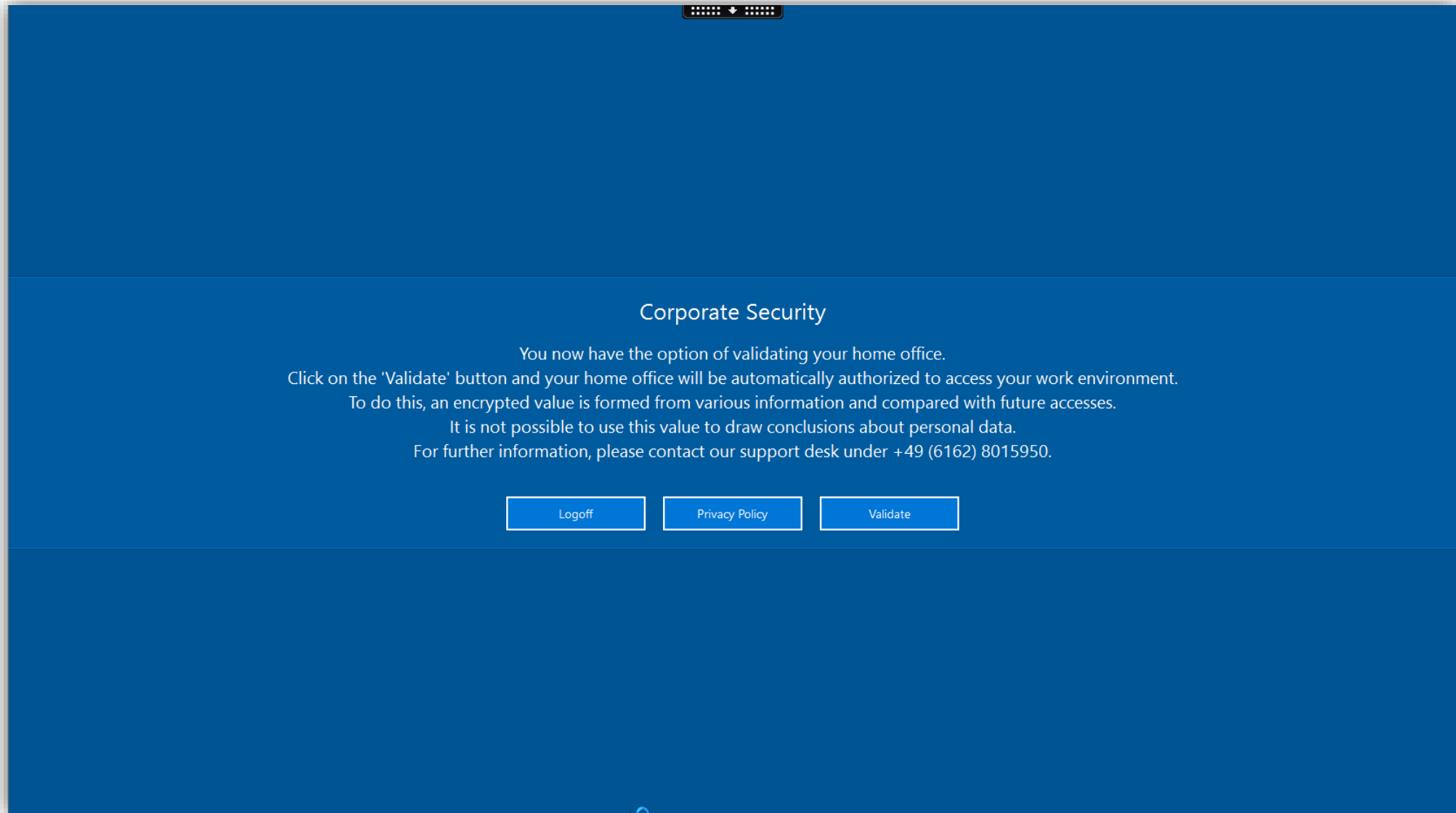
Very High

**Home Office Conditional Access - Compliance Check**  
Applies conditional shell access policies for home office users.

High

**Home Office Conditional Access - Validate and Detect**  
Applies conditional shell access policies for home office users.

# Step 2: Validate and Detect

A screenshot of a web application interface with a dark blue background. At the top center, there is a small black rectangular box containing a white downward-pointing arrow and several small white dots. Below this, the text 'Corporate Security' is centered in white. Underneath, there are four lines of white text explaining the validation process. At the bottom, there are three white rectangular buttons with blue text: 'Logoff', 'Privacy Policy', and 'Validate'.

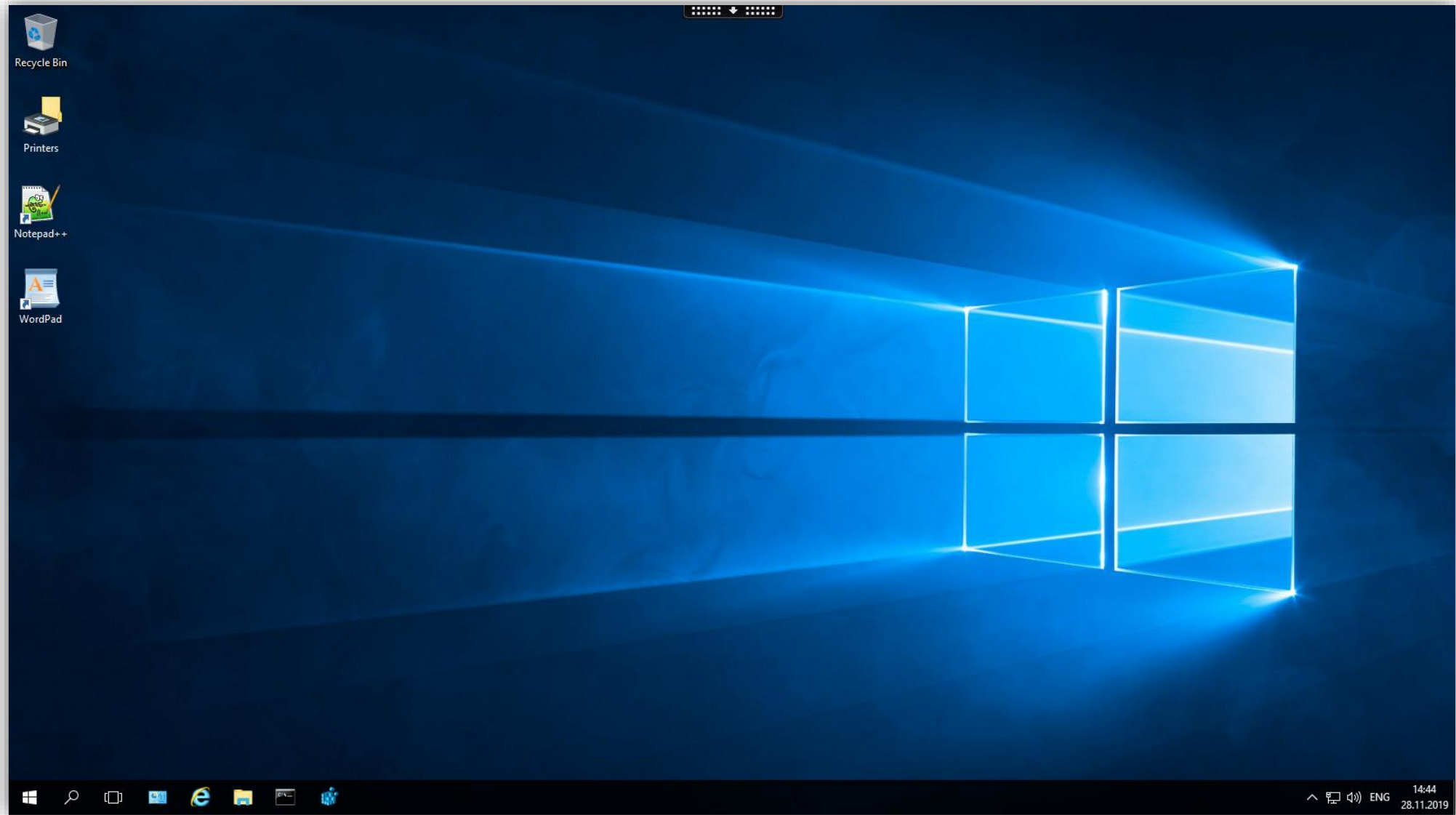
Corporate Security

You now have the option of validating your home office.  
Click on the 'Validate' button and your home office will be automatically authorized to access your work environment.  
To do this, an encrypted value is formed from various information and compared with future accesses.  
It is not possible to use this value to draw conclusions about personal data.  
For further information, please contact our support desk under +49 (6162) 8015950.

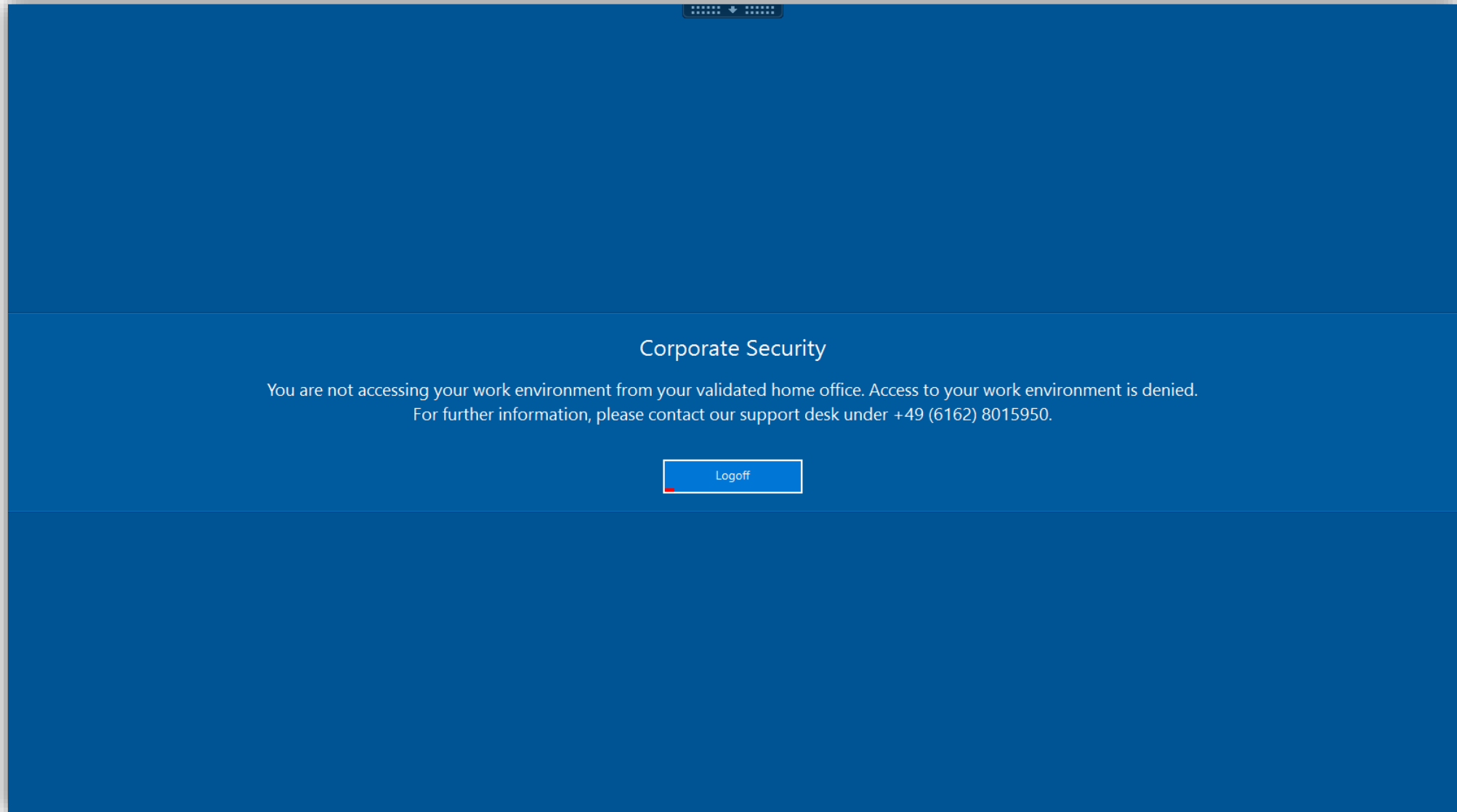
Logoff   Privacy Policy   Validate



# Step 2: Validate and Detect



# Step 2: Validate and Detect



# deviceTRUST 19.4 Templates



The screenshot shows the 'deviceTRUST Console (Local Computer Policy)' interface. A central dialog box titled 'Import from Template' is open, displaying a list of available templates. The 'Home Office' template is highlighted with a red rectangular border. The list includes:

- deviceTRUST Client**: Ensures that the deviceTRUST Client is available on the remote device.
- Home Office**: Allows external users to validate a Home Office location for their remote device.
- Microsoft Office Licensed Device**: Controls access to Microsoft Office using either Microsoft AppLocker or FSLogix App Masking using the BIOS Serial Number, OS ID or NetBIOS Name of the remote device.
- Microsoft Project Licensed Device**: Controls access to Microsoft Project using either Microsoft AppLocker or FSLogix App Masking using the BIOS Serial Number, OS ID or NetBIOS Name of the remote device.
- Microsoft Visio Licensed Device**: Controls access to Microsoft Visio using either Microsoft AppLocker or FSLogix App Masking using the BIOS Serial Number, OS ID or NetBIOS Name of the remote device.
- Power Supply**: Displays a notification to the user when the remote device is low on power.
- Previous Country**: Determines the country where the remote device is located, using for a limited time the previous country of the remote device when the location is unavailable.
- Printer Management based on IP address**: Connects network printers and defines a default printer based on the IP address of the remote device.
- Printer Management based on NetBIOS name**: Connects network printers and defines a default printer based on the NetBIOS name of the remote device.
- Remote Controlled**: Prevents access to the session when the remote device is remote controlled. Requires the 'deviceTRUST Client' template.
- Remote Device Information**: Provides a set of contexts describing various information about the remote device.
- Remoting Performance**: Displays a notification to the user when the quality of the remote connection is poor.
- Secure Screen Saver**: Ensures remote devices have a secure screen saver enabled.