



# WORLD WIDE TECHNOLOGY AND DUO TRUSTED ACCESS PLATFORM

Streamlining  
Federal Agency  
Non-CAC MFA  
Capability Within  
Enterprise Access  
Management  
Services

## THE CHALLENGE

Federal agencies like the DoD are exploring ways to implement and expand Continuity of Operation (COOP) programs by integrating personally-owned devices. The remote workforce was growing rapidly even before the current public health crisis. This crisis and other current events are increasing the demand for Government-furnished Equipment (GFE) and constricting its availability to the workforce.

One of the most pressing consequences of the present scenario is that agencies are challenged by increased demand for mobile-driven second-factor authentication for enterprise logins. Like their private sector counterparts, Government agencies require a secure and user-friendly self-service method to provide proof of possession of a registered – but unmanaged – smart device to access systems with a password or other non-Common Access Card (non-CAC) second factors.

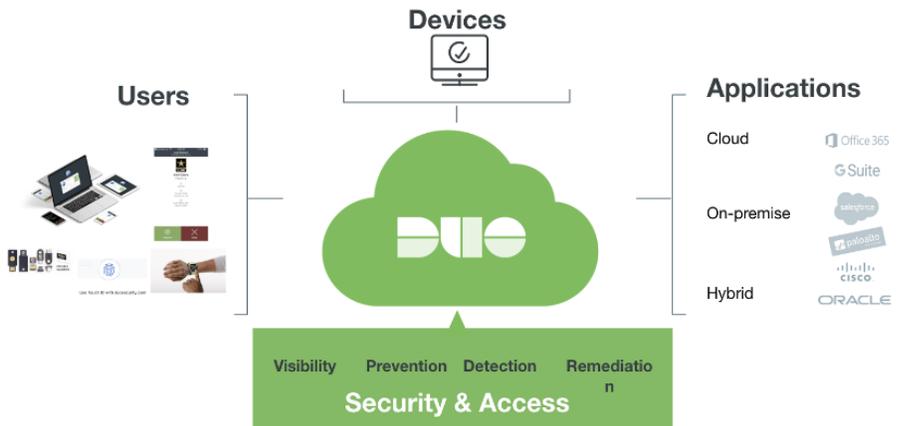
More specifically, agencies like the DoD are seeking a secure Multi-factor Authentication (MFA) solution to augment CAC authentication for Soldiers without GFE – including Individual Ready Reserve Soldiers without CACs and other non-CAC eligible mission partners who need to access IT resources at critical times.

## THE SOLUTION: WORLD WIDE TECHNOLOGY (WWT) AND DUO TRUSTED ACCESS PLATFORM

In response to this critical need, WWT and Duo combined our capabilities to offer a simple, scalable and secure solution to a variety of federal agencies. Our solution establishes a non-CAC MFA capability within any organization's Enterprise Access Management Services.

The key is offering the right person, with the right device the right amount of access to the network in order for them to continue to operate and perform their mission, as shown below. The Duo Trusted Access platform provides the integrated solution and the building blocks for each and every access attempt to an organization's enterprise resources.

## EASY AND EFFECTIVE - RIGHT USER. RIGHT DEVICE. RIGHT APPLICATION.



## ABOUT WWT

World Wide Technology (WWT) is a technology solution provider with more than USD 11 billion in annual revenue that provides innovative technology and supply chain solutions to large public and private organizations around the globe. While most companies talk about delivering business and technology outcomes, WWT does it. Based in St. Louis, WWT employs more than 6,000 people and operates over 4 million square feet of warehousing, distribution and integration space at its [Integration Centers](#) around the world.

**World Wide Technology**  
**1 World Wide Way**  
**St. Louis, MO 63146**

[wwt.com/federal](http://wwt.com/federal)

## HOW DUO BUILDING BLOCKS WORK

Simple, scalable and secure are the hallmarks of the best process for enabling a remote workforce with personal devices. The Duo Trusted Access platform achieves all of these objectives – and does so at speed and scale. Additionally, the Duo platform evolved from a clear understanding of the effort required to deploy and administer this process. The platform also minimizes risk by validating a user's identity and the trustworthiness of their device, while evaluating context for each and every access attempt. The Duo platform's five-step process is described below.

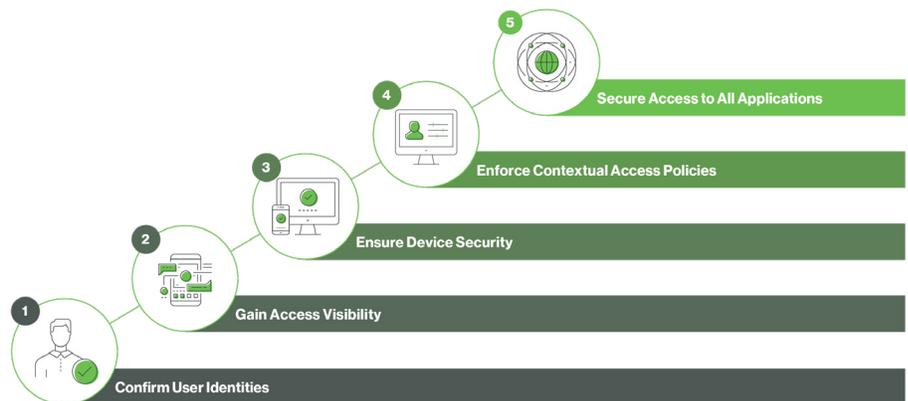
**1. Establish User Trust** - Verify the identity of all users with easy-to-use and effective, strong multi-factor authentication before granting access to enterprise applications and resources.

**2. Gain Visibility Into Devices and Activity** - Gain visibility into every device used to access enterprise applications, whether the device is enterprise managed or unmanaged, and without the use of onerous device management agents.

**3. Ensure Device Trustworthiness** - Inspect all devices used to access enterprise applications and resources in real time, at the time of access, to determine their current security posture and trustworthiness.

**4. Enforce Adaptive Policies** – Provide the ability to use adaptable trust algorithms to make real-time access decisions. Factors such as time, location, reputation and many other attributes can be combined into Duo's policy engine at the time the access request is made.

**5. Enable Secure Access to all Applications** - Grant users secure access to all protected applications (on-premises or cloud-based) through a uniform, frictionless interface accessible from anywhere. Duo inserts into the authentication workflow for all applications and resources after primary authentication has been completed successfully.



## A STRAIGHTFORWARD WAY TO ACQUIRE THIS SOLUTION

Agencies with a diverse user population, such as Armed Services, federal agencies, mission partners, first responders, foreign nationals and academia that require secure access to enterprise information technology (IT) resources for training and mission operations will immediately benefit from implementing the Duo Trusted Access platform. These agencies can acquire this solution by leveraging a successful OTA initiative with the Army PEO-EIS. WWT in conjunction with Duo can provide additional information, use cases and enterprise specific workshops to help agencies achieve a secure Multi-factor Authentication (MFA) solution. Contact the numbers below for more information.