SOLUTION SHEET

TrafficAuth-Gateway

Secure connectivity for traffic management networks

Connect protected transportation infrastructure to trusted SCMS and Network V2X services through a controlled, outbound access point—with fewer changes to the Traffic Management Center network.

Connect with less network disruption

Traffic Management Center (TMC) networks support critical operations, but established configurations, strict security policies, and lengthy approval processes can make every new external connection a challenge.

TrafficAuth-Gateway gives approved roadside units, roadside processors, and TMC applications a shared path to specifically authorized external resources. Preconfigured for TrafficAuth-SCMS and Network V2X services, it simplifies connectivity while keeping the agency in control of its network boundary.

CUSTOMER BENEFITS

Simplify external access. Consolidate approved V2X communications through one gateway. Reduce the network changes needed to bring connected infrastructure online.

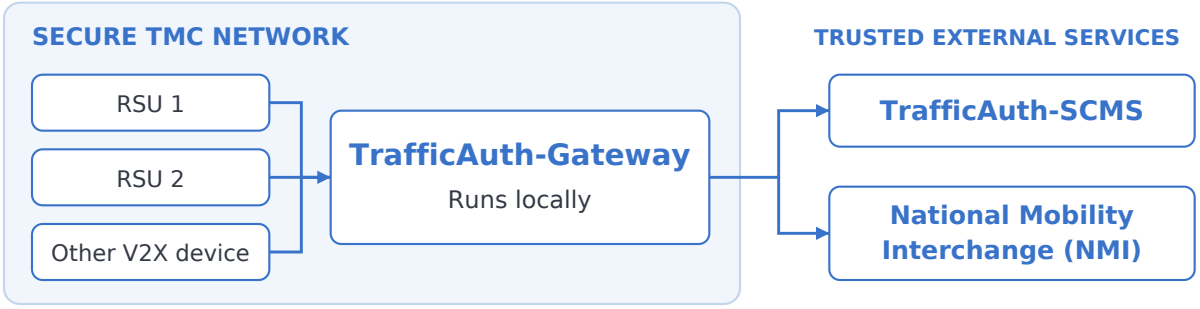
Keep access focused. Connect approved devices to known service destinations without granting unrestricted internet access. Service connections originate inside the agency network, with no requirement to accept unsolicited inbound connections.

Start with V2X ready configuration. Use service configurations prepared for SCMS and Network V2X workflows. OmniTrust coordinates setup and commissioning with your team.

A controlled path to trusted services

TrafficAuth-Gateway is designed to provide a controlled connection into a secure back-office service environment operated by OmniTrust, giving agencies a consistent way to reach required resources as their connected transportation programs grow.

Secure access through a local gateway



Arrows show connections initiated inside the TMC network.



Built for connected transportation

TrafficAuth-Gateway brings service connectivity together in a dedicated access point for transportation operations. It complements existing agency firewalls and security policies with configuration tailored to V2X deployments.

SCMS connectivity

Connect approved V2X devices to TrafficAuth-SCMS for certificate management and trust services, supporting digitally signed V2X communications.

Network V2X exchange

Connect devices and applications to the National Mobility Interchange (NMI) to publish and subscribe to transportation data. Enable the connectivity needed for signal timing and intersection geometry distribution, signal priority and preemption messaging, and traveler alerts.

The gateway provides the connection; TrafficAuth services and participating devices perform the application functions.

A simpler path to deployment

External service access typically requires agencies to identify destinations, develop rules, and resolve device connectivity requirements. TrafficAuth-Gateway brings these tasks together in a solution configured for the V2X services your deployment needs.

Plan. OmniTrust works with agency IT and operations staff to identify approved clients and required services, then prepare the gateway configuration.

Connect. Validate representative device connections and begin with a small group of devices before expanding through a repeatable onboarding process.

Operate. The agency retains control of its network and access approvals. OmniTrust supports gateway configuration, maintenance, and troubleshooting throughout the deployment lifecycle.

Connect your next V2X deployment

Work with OmniTrust to define the approved devices and service connections for your TMC network and plan a controlled rollout of TrafficAuth-Gateway.

ABOUT TRAFFICAUTH

TrafficAuth, powered by OmniTrust, supports trusted communications across vehicles, roadside infrastructure, and traffic systems. Its SCMS and Network V2X services help infrastructure operators deploy connected transportation applications with authenticated participants and standards-based messaging.

trafficauth.com

© 2026 OmniTrust Security, all rights reserved.