



Secure Gateway Access

Beginning in 2018, many OEMs began equipping vehicles with Secure Gateway Modules. In the most basic form, a Secure Gateway Module is a firewall designed to prevent unauthorized access to critical vehicle electronic systems. Secure Gateway Modules help prevent damage to vehicles from non-compliant tools, or access to critical safety systems, such as ADAS Controls, Engine, Steering, and even Brake Controls.

Secure Gateway access falls into two categories:

- › Access through an Independent Authentication Service, such as AutoAuth®
- › Access directly on tool with license agreements between the OEM and Bosch, using SingleKey ID®

 **Stable WiFi network:** Due to the nature of accessing Secure Gateway Modules it is recommended to have a stable WiFi network in your shop so the Secure Gateway Module can be unlocked properly.

 Currently most OEMs use Secure Gateway Modules in their vehicle systems, the only exceptions are BMW, GM, and Toyota.

 Hunter strives to simplify the complexities of Secure Gateway Access by including SGW access to many OEMs at no extra charge with an active ADASLink® subscription. Currently only Stellantis* and Nissan vehicles require a third party subscription through AutoAuth®.

See reverse side for access login information.

*Stellantis brand vehicles include Alfa Romeo, Chrysler, Dodge, FIAT, Jeep, Maserati, and RAM.

OEM	Model year Secure Gateway introduced	Included with active ADASLink® subscription	Wi-Fi connection required to unlock
Stellantis	2018+	AutoAuth REQUIRED	Yes
Nissan	2020+	AutoAuth REQUIRED	Yes
Mercedes	2020+	Yes	Yes
VW/Audi	2023+	Yes	Yes
Porsche	2018+	Yes	Yes
Hyundai/Kia/Genesis	2018+	Yes	Yes
Ford	2018+	Yes	Yes
Honda	2022+	Yes	No
Mitsubishi	2022+	Yes	No
Subaru	2020+	Yes	No
Volvo	2021+	Yes	No
Polestar	2021+	ADASLink® RDS*	Yes – via RDS
Jaguar / Land Rover	2026+	ADASLink® RDS*	Yes – via RDS
Mazda	Coming Soon	ADASLink® RDS*	Yes – via RDS
GM	Not Equipped	Not Required	Not Required
Toyota	Not Equipped	Not Required	Not Required
BMW	Not Equipped	Not Required	Not Required

*ADASLink® RDS (Remote Diagnostic Service)



Secure Gateway Access *(continued)*



Secure Gateway access through AutoAuth®

AutoAuth® is the independent authentication service required by Nissan and Stellantis (Alfa Romeo, Chrysler, Dodge, FIAT, Jeep, Maserati, and RAM) to access the Secure Gateway Module and perform required services.

Hunter Engineering Company has worked with FCA US in getting our ADASLink® scan tool approved and certified for use on FCA vehicles, effectively providing independent shops and their technicians the ability to work within these security features and perform the necessary diagnostic procedures.



NEW USERS: Begin the registration process by going to the AutoAuth website (autoauth.com). Click **Register** to create your account. Once you are registered, you will also need to set up a Shop Account.

ACTIVE USERS: If you already have an AutoAuth account and need to add a tool, log in to your Shop Account. Select **Manage Tools**.

Identify the serial number for your device via **Settings > Software Information**. Pay careful attention to the difference between the number "0" and letter "O".

Click **Add Tools**.

- Use the drop-down menu to select **Hunter** as the manufacturer and **All Models** as the Tool Model.
- Enter the serial number.
- Click **Add Tool**.

IMPORTANT: Using any registered device, attempts to perform a secured diagnostic service using AutoAuth, will require entry of AutoAuth credentials.



COMPLETE
LOGIN DETAILS



Secure Gateway access using SingleKey ID®

SingleKey ID® is a unified single-sign-on platform used by Bosch and partner brands to access websites, shops, apps, and services.

Once users have a SingleKey ID account, always start the login process from the Hunter ADASLink® scan tool. Avoid accessing the SingleKey ID login page via browser bookmarks



SingleKey ID

NEW USERS: Begin the registration process by going to the SingleKey ID website (singlekey-id.com) Click **Create SingleKey ID Now** and follow prompts to create user account. Provide an email address or mobile phone number that is not yet signed up with SingleKey ID.

User passwords must contain at least: 1 digit, 1 upper- and lowercase character, 8 characters. To separate a private account from a business account, users are currently required to sign up two different SingleKey ID user identities.

ACTIVE USERS: Login from the Hunter ADASLink® scan tool. Users have an option during the login process when entering the password to click the checkbox "Stay logged in" which keeps you logged in for 30 days for the specific device where the login process was conducted.



SIGN-UP
DETAILS