

ISTA: Release notes programming car 4.34.4x (ISTA/P 3.70.0)

The release notes contain information on known problems when handling passenger cars with ISTA.



Release notes

If this software version is not yet available to you, please wait for information from your market responsible.

ISTA release

ISTA	4.xx
{ISTA Service Data}	4.34.40
ISTA/P	3.70.0

General notes

With the introduction of ISTA 4, vehicle programming functionality was integrated into ISTA.

The following series can be treated with ISTA/P:

- E-series

The following series can be treated with ISTA 4:

- F, G and I series

These release notes contain information for both programming systems.

The release notes list all known and currently open errors and possible workarounds that are decisive for the retail organization. If errors also occur on the vehicle, please contact technical support. In particular in the following cases:

- Vehicle-related programming errors/coding errors and enabling errors
- functional faults on the vehicle

With ISTA 4, feedback concerning vehicle programming can now also be transmitted directly to BMW AG. When selecting the "Feedback" icon (envelope icon), the feedback mask with input fields is displayed.

If a new error profile is recorded in a release, this is **marked with *NEW*** in the heading. In the subsequent release, there is no labelling on this topic.

What's New (General)

Among other things, the following interesting new features are included.

New models are treatable

Use: The new vehicles (I20, G26, G42, G83, U06) are treatable.

Overview of the included I-levels

New or updated I-levels on this ISTA version are **marked in BOLD**.

F, G, I series (ISTA 4)

Series group	I level
{F001 (F0x, RR4, RR5, RR6)}	{F001-22-03-510}
{F010 (F06, F1x)}	{F010-22-03-510}
{F020 (F2x, F3x, F80, F82, F83, F87)}	{F020-22-03-540}
{F025 (F15, F16, F25, F26, F85, F86)}	{F025-22-03-510}
{F056 (F39, F4x, F5x, F6x)}	{F056-22-03-540}
{I001 (I01, I12, I15)}	{I001-22-03-526}
{I020 (I20)}	{I020-22-03-540}
{RR21 (RR21, RR22)}	{RR21-22-03-535}
{S15A (G01, G02, G1x, G3x, RR1x, RR31, F90, F97, F98)}	{S15A-22-03-540}
{S15C (G08, G38)}	{S15C-22-03-540}
{S18A (G05, G06, G07, G14, G15, G16, G18, G20, G21, G22, G23, G26, G28, G29, G42, G80, G82, G83, F40, F44, F91, F92, F93, F95, F96)}	{S18A-22-03-540}
{U006 (U06)}	{U006-22-03-540}

I levels correspond to the {ISTA Service Data} version on the cover page.

E-series (ISTA/P)

Series group	I level
{E065 (E65, E66)}	{E065-17-11-545}
{E060 (E60, E61, E63, E64)}	{E060-16-11-500}
{E070 (E70, E71, E72)}	{E070-16-11-500}
{E89x (E81, E82, E84, E87, E88, E89, E90, E91, E92, E93)}	{E89x-21-07-550}
{R056 (R55, R56, R57, R58, R59, R60, R61)}	{R056-17-03-504}
{RR01 (RR1, RR2, RR3)}	{RR01-22-03-500}

Explanations of the I levels

PUMA measures/service solutions or similar documents sometimes refer to an I level to solve a problem. In this case, it is important to know which ISTA release includes the I level.

The naming of the I level can be used to find out whether it

1. is available on the latest ISTA release,
2. was already included in a previous ISTA release, or
3. will be made available on a future ISTA release.

Series network, e.g. **F020** - year **2017** - Month **(3, 7, or 11)** - Version (**>= 500**)

Assume the current release contains:	{S15A-17-03-506}
In this case, the following I-level is not yet available:	{S15A-17-07-501}
Then this I-level was already on an older ISTA release:	{S15A-16-11-503}
Then this I-level was already on an older ISTA release:	{S15A-17-03-505}

innovations

Among other things, the following interesting new features are included.

New models are treatable

Use: The new vehicles(G18) are treatable.

Innovations - Secure coding

With the introduction of the(I20) and the following models, a new tamper protection - secure coding - is introduced.

Up to now, the coding data for programming ISTA has been calculated and written to the ECUs.

With secure coding, the required coding data is calculated in a BMW backend and sent to ISTA. ISTA then writes the data to the ECUs.

Automatic process

With ISTA, this process can only run **automatically as part of programming** if the ISPI Admin Client is correctly configured and an online connection is available to the BMW backend.

The necessary settings for the ISPI Admin Client are described in the ISPI Administrator manual (application: ISPI Admin Client (administration area)/ISPI Admin Client: Features/ISPI Admin Client: certification management).

BMW Group internal location: The S-Gate environment (internal locations) must be set in the ISPI Admin Client.

Manual process

If the prerequisites for the automatic process are not met, ISTA automatically cancels the action plan and a file dialog for saving the automatically generated file of type(SecureCodingNCDCalculationRequest_VIN_XXX.json) is open.

This file must be sent to technical support via PUMA/tsara.

Technical support provides a validated coding data set based on the above file. This must then be imported into ISTA.

The coding record can be imported as follows:

1. Go to the "(Vehicle modification)" tab and select(Secure coding)(Secure Coding)".

Operations	Vehicle information	Vehicle management	Service plan	Favourites	Workshop/ Operating fluids	Measuring devices
Repair/ maintenance	Troubleshooting	Service functions	Software update	Control Unit Replacement	Vehicle modification	
Retrofit	Conversion	Conversion (coding only)	Removal of Re- trofit/Conversion	Remove conver- sion (coding only)	Immediate actions	

Designation	Selection
Import vehicle order	<input type="checkbox"/>
Import encoding data record	<input type="checkbox"/>
Import Secure Feature Activation customer function	<input type="checkbox"/>
Initialisation of component protection	<input type="checkbox"/>
Import secure token	<input type="checkbox"/>
Control unit validation	<input type="checkbox"/>

2. A file dialog opens for importing the file provided by technical support (type \$yyyy-MM-DD_VIN.zip). Confirm your selection.

3. File is checked. ISTA then automatically calculates an action plan and switches to the "Action plan" tab.

4. Review the calculated action plan and then execute it.

What's New - Secure Token

With the introduction of the I20 and the following models, the use of the Secure Token will be expanded.

The Secure Token is a further development of activation codes.

Compared to an activation code, it offers the advantage of being controlled via the BMW backend even without an ISTA session.

This makes it possible, for example, to activate vehicle functions via the BMW ConnectedDrive Store.

Secure tokens can be used for various applications:

- Secure feature activation - to control customer functions, such as traffic sign recognition, etc.
- Locking Configuration Switch - for controlling ECU functions in the event of an ECU replacement
- Theft protection components - the extension of component protection to further components and control devices in the event of a control unit replacement
- Diagnostics - to activate ECU mode or functions

The secure token becomes relevant when an affected ECU is replaced.

As before, the software functions of a new part control device are set to the vehicle by means of coding.

In the future, some of the software functions will be protected by the locking configuration switch.

Customer functions are activated by means of Secure Feature Activation.

Component theft protection ensures that the new parts control unit functions in the vehicle.

The required secure tokens are requested by a BMW backend and written to the ECUs by ISTA.

The I20 uses both the classic activation codes and secure tokens.

Automatic process

ISTA performs this process automatically, provided that the affected workshop systems (ISPI Admin Client) are correct are configured and there is an online connection to the BMW backend.

Operations	Vehicle information	Vehicle management	Service plan	Favourites	Workshop/ Operating fluids	Measuring devices
Repair/ Maintenance	Troubleshooting	Service functions	Software update	Control Unit Replacement	Vehicle modification	
Before Replacement	After Replacement					

Short name	Description	Replaced
ACSM	Crash safety module	<input type="checkbox"/>
AHM	Trailer module	<input type="checkbox"/>
AL	Active steering	<input type="checkbox"/>
AMPT	Top HiFi amplifier	<input type="checkbox"/>
BDC	Body Domain Controller	<input type="checkbox"/>
CON	Controller	<input type="checkbox"/>
DDE	Digital diesel electronics	<input type="checkbox"/>
DSC	Dynamic Stability Control	<input type="checkbox"/>
EDC	Vertical Dynamics Management	<input type="checkbox"/>
EGS	Electronic transmission control	<input type="checkbox"/>
FHC	Electronic ride height control	<input type="checkbox"/>

Hint: To finalize the replacement of the already installed ECU, select the corresponding control unit.

Display measures plan

To do this, select the affected ECU in the "(After Replacement)" tab and execute the action plan.

ISTA must be enabled to apply for vehicle certificates in order to retrieve secure tokens.

The necessary settings for the ISPI Admin Client are described in the ISPI Administrator manual (application: ISPI Admin Client (administration area)/ISPI Admin Client: Features/ISPI Admin Client: certification management).

BMW Group internal location: The S-Gate environment (internal locations) must be set in the ISPI Admin Client.

Manual process

If the prerequisites for the automatic process are not met, the secure token must be imported with the help of technical support.

The process is similar to ECU validation.

If ISTA could not automatically import the secure token, a warning message will be displayed.

 **Warning!**

Automatic Secure Token download not possible or failed.

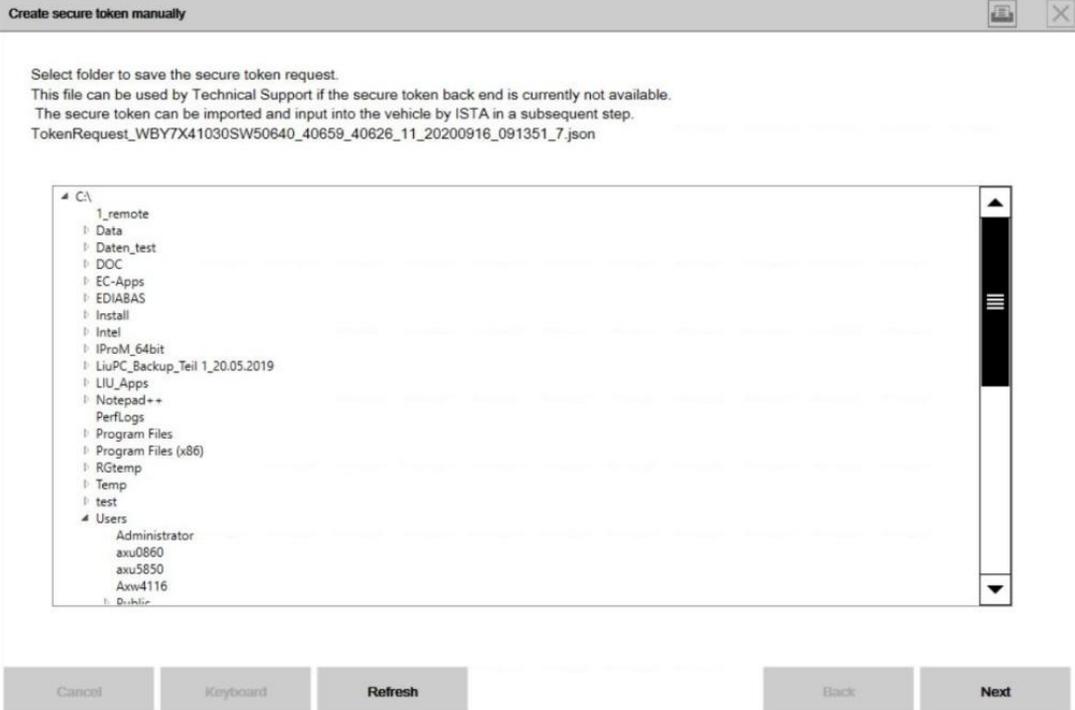
Secure token download and activation after control unit exchange (SME) und (EME) und (CCU) is mandatory!

The next steps in the procedure are as follows:

- Continue with the manual generation of the secure token request file as part of this measures plan.

Exporting secure tokens from ISTA

When you select the "OK" button, ISTA generates the required ZIP archive in the format(TokenRequest_VIN17_DealerData1_DealerData2_OutletNo_YYYYMMDD_HHMMSS.zip) and opens a file dialog for saving. This file must later be sent to technical support via PUMA or TSARA.



The session can be ended if necessary.

TSARA

Send the saved ZIP archive to technical support using PUMA/tsara.

Technical support will send you back a validated version of the ZIP archive in the format(TokenRequest_VIN17_response.zip) for the affected vehicle. This is then required by ISTA.

Importing Secure Tokens into ISTA

Connect to the vehicle.

To import the ZIP archive, select "(Import secure token)" in the "(Immediate actions)" tab.

Operations	Vehicle information	Vehicle management	Service plan	Favourites	Workshop/ Operating fluids	Measuring devices
Repair/ maintenance	Troubleshooting	Service functions	Software update	Control Unit Replacement	Vehicle modification	
Retrofit	Conversion	Conversion (coding only)	Removal of Re- trofit/Conversion	Remove conver- sion (coding only)	Immediate actions	

Designation	Selection
Control unit validation	<input type="checkbox"/>
Import secure token	<input type="checkbox"/>
Import vehicle order	<input type="checkbox"/>
Initialisation of head unit component protection	<input type="checkbox"/>

Select and confirm the file(TokenRequest_VIN17_response.zip) in the file dialog.

When the ZIP archive has been read successfully, ISTA automatically switches to the ECU exchange/after replacement tab.

Mark the affected control unit there as replaced.

Calculate and execute the action plan.

Innovations - Components theft protection

With the introduction of the I20 and the following models, a new tamper protection - the components theft protection - is introduced.

The component theft protection is intended to prevent the theft of vehicle components.

This is achieved by coupling the components to the central control unit (BCP) of the vehicle.

It is a further development of component protection. Component protection couples the head unit to the central control unit (BDC) and works with enable codes.

In the case of I20 are coupled: Gear selector, controller, BZM, the head unit.

If one or more of the protected components are exchanged, the coupling with the (BCP) reinitialized.

This is done with the help of secure tokens.

Automatic initialization of component theft protection when replacing a coupled component

After installing the new part and instructing it "after exchange" in ISTA, the required secure tokens are automatically downloaded and activated.

Manual process for initializing the anti-theft protection components

If ISTA cannot reach the BMW backend system, the secure tokens can be imported into ISTA manually.

The necessary zip archive is provided by technical support.

To import, go to the "(Immediate actions)" tab and select "(Initialisation of component protection)" (Initialization of component protection)".

Operations	Vehicle information	Vehicle management	Service plan	Favourites	Workshop/ Operating fluids	Measuring devices
Repair/ maintenance	Troubleshooting	Service functions	Software update	Control Unit Replacement	Vehicle modification	
Retrofit	Conversion	Conversion (coding only)	Removal of Re- trofit/Conversion	Remove conver- sion (coding only)	Immediate actions	

Designation	Selection
Import vehicle order	<input type="checkbox"/>
Secure coding - coding data calculation	<input type="checkbox"/>
Initialisation of component protection	<input type="checkbox"/>
Import secure token	<input type="checkbox"/>
Control unit validation	<input type="checkbox"/>

Select the zip archive in the file explorer and follow the instructions.

Component protection

Component protection is used to couple the head unit with the vehicle(BDC) (BDC). If a coupled head unit is installed in another vehicle, it discards the activation codes and the functions such as navigation, etc. are no longer available. This is intended to prevent the theft of head units.

Component protection has been applied to all vehicles with(BDC) in combination with the head units HU-H2 ((NBT Evo)), HU-B2 ((Entry Evo)) and HU-H3 ((MGU)) were introduced.

If the(BDC) must be reset in order(BDC) (BDC).

A release code is required for resetting.

Automatic unlocking of component protection when replacing the(BDC)

The activation code required to unlock component protection is(BDC) (BDC). After installing the new part(BDC) and instructing it "after exchange" in ISTA, the activation code is downloaded and activated.

Manual process to unlock component protection

The manual process is documented in the ISTA User's Guide, chapter Immediate Actions.

The user manual can be downloaded in ISTA using the "?" can be called.

Known faults F, G, I, U series

ECUs cannot be programmed((Not Executable))

Problem description:

The MPAD or indoor camera((IRK)) cannot be programmed (result(Not Executable)).

Affected series:

vehicles(U06, I20).

measure/ workaround:

- 1) Configure ICOM on DHCP (see also COMPASS #4308).
- 2) Activate WLAN on ISTA computer to enable an Internet connection.
- 3) Connect ICOM directly to ISTA computer using a network cable.
- 4) Start session and do programming.

If the programming still fails with the error pattern:

- 1) End the session and let the vehicle fall asleep.
- 2) Reconnect ICOM via workshop network.
- 3) Start ISTA session and do programming.

If the programming still fails with the error pattern:

- Contact technical support for an IRAP session.

Bug fixed until:

With ICOM firmware 04-22-10

Internal ID: 35741

Programming is not possible after replacing the FEM

Problem description:

No programming/coding is possible after replacing the FEM ECU.

The vehicle cannot be identified using ISTA.

Affected series:

Vehicles {F2x, F3x, F80, F82, F83, F87} after replacing the FEM.

measure/ workaround:

Contact technical support for an IRAP meeting.

Bug fixed until:

Expected ISTA 4.35.1x

Internal ID: 35469

Programming aborts with ICOM Next

Problem description:

During programming, programming of various ECUs is repeatedly aborts.

Affected series:

ICOM Next with firmware{3-15-08}.

measure/ workaround:

Use an ICOM A with firmware {3-15-09}.

Configure ICOM on DHCP (see also COMPASS #4308).

Bug fixed until:

With ICOM firmware 04-22-10

Internal ID: 35260

U06 - FZD cannot be programmed

Problem description:

During programming, programming aborts occur repeatedly at the Dach function center{FZD}.

Affected series:

Vehicle{U06} with optional equipment{4NR} and construction status 11/2021.

measure/ workaround:

Connect the ICOM directly to the ISTA computer using a network cable.

Carry out programming.

Bug fixed until:

The problem no longer occurs with vehicles built from 03/2022 onwards.

Internal ID: -

Notes on individual data actions

Problem description:

If necessary, after vehicle programming, actions for restoring individual data are completed with the result warning and scheduled again by ISTA in the final work.

The behavior can also occur if no control device has been replaced.

The background is the updating of the programming functions included in ISTA for future derivatives.

Affected series:

All series.

measure/ workaround:

The actions regarding the individual data can be ignored.

Bug fixed until:

Currently open.

Internal ID: 31125, 31202, 31203, 31204, 31784

Note on BDC exchange or programming abort gateway ECUs

The exchange of the body domain controller is supported again with ISTA 4.09.1x.

Problem description:

When executing the special action plan in the event of a{BDC} exchange or due to a programming termination of the gateway ECU, the following pop-ups occur several times:

- When prompted to switch on the ignition

- {SYS-0012 Identification Error}
- Connection to control unit{Unknown} failed

Affected series:

Vehicles with the control units(FEM) or(BDC).

measure/ workaround:

Pop-ups confirm until the special action plan has been carried out.

Bug fixed until:

Currently still open.

Internal ID: 21984, 21976, 21977

Known faults E-series (ISTA/P)

Vehicle order import fails due to antivirus software and firewall

Attention!

In isolated cases, the vehicle order import fails due to installed security software (antivirus software or firewall). After the start of the session, vehicle identification with ISTA/P fails. (BMW internal offices are not affected by the error)

measure/ workaround:

For further details, see compass entry 51219