

SIMATIC

SIMATIC Unified AR App for iOS

Application manual

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

SIEMENS

SIMATIC Unified AR

App for iOS

Application manual

Table of contents

1	Data Privacy Notice	4
1.1	Categories of personal data processed, and purpose of the processing	4
1.2	Legal basis of the processing	4
1.3	Cookies.....	5
1.4	Transfer and disclosure of personal data	5
1.5	Retention periods.....	6
1.6	Your rights	6
1.7	Threat and Risk Assessment	6
1.8	Contact.....	6
1.9	Usage by children	7
1.10	Data security.....	7
1.11	Only for US residents.....	7
2	SIMATIC Unified AR	8
2.1	Configuring barcodes	8
2.2	The Composition menu.....	9
2.3	The Screen menu	9
2.4	The System menu	10
2.4.1	Certificates.....	10
2.4.2	System authentication	10
2.4.3	Operating systems in full-screen mode	11
2.5	Scanning barcodes.....	11
2.6	Resetting the AR view.....	11
2.7	Additional information and feedback	11
2.8	System requirements	11

1 Data Privacy Notice

Protecting your personal data is a priority for Siemens AG, Werner-von-Siemens-Strasse 1, 80333 Munich, Germany ("Siemens"). This is why Siemens uses Unified AR ("app") in accordance with the applicable legislation governing data privacy and data security.

1.1 Categories of personal data processed, and purpose of the processing

Siemens processes the following personal data about you when you visit us and use the app:

User content:

- **User videos**, provided that permission has been granted,
- **Other user-generated content**: Login data (on a voluntary basis, stored on the device)

We process your personal data for the following purposes:

- **App functionality**
- **Use of the app**, e.g. to authenticate the user's identity, activate functions

We only process your personal data if we are entitled to do so by the existing legislation.

1.2 Legal basis of the processing

The General Data Protection Regulation requires us to provide you with information on the legal basis of the processing of your personal data.

Unless specifically stated otherwise when personal data are collected, the legal basis for data processing is:

- Exercising our rights and performing our obligations under any contract we make with you (Article 6 (1) (b) of the General Data Protection Regulation) ("**Contract Performance**"),
- Compliance with our legal obligations (Article 6 (1) (c) of the General Data Protection Regulation), ("**Compliance with Legal Obligations**") or
- Legitimate interests pursued by us (Article 6 (1) (f) of the General Data Protection Regulation) ("**Legitimate Interest in Processing**"). The legitimate interest pursued by us in relation to our use of your personal data is the efficient performance or management of (i) your use of the Online Offerings and (ii) our business relationship with you. Where the below table states that we rely on our legitimate interests for a given purpose, we are of the opinion that our legitimate interest is not overridden by your interests and rights or freedoms, given (i) the regular reviews and related documentation of the processing activities described herein, (ii) the protection of your personal data by our data privacy processes, including our Binding Corporate Rules on the Protection of Personal Data, (iii) the transparency we provide on the processing activity, and (iv) the rights you have in relation to the processing activity.

If you wish to obtain further information on this balancing test approach, please contact our Data Privacy Organization at: dataprotection@siemens.com.

In some cases, we may ask if you consent to the relevant use of your personal data. In such cases, the legal basis for Siemens processing this personal data may be that you have consented (Article 6 (1) (a) General Data Protection Regulation).

1.3 Cookies

This app may use cookies (small files that contain specific information stored on your device). If we use these cookies without your consent, they must be absolutely essential for you to use specific functionalities of an Online Offering or to provide you with a service that you have requested via the Online Offering. Other cookies (e.g. cookies for marketing purposes) are only used if you have granted consent.

1.4 Transfer and disclosure of personal data

Siemens may transfer or disclose your personal data, for the purposes mentioned above, to:

- Other affiliated companies or third parties, e.g. sales partners or suppliers, in connection with your use of the Online Offerings or our business relationship with you;
- Third parties that provide IT services for us and process this data solely for the purpose of such services (e.g. hosting or IT maintenance and support services); and
- Third parties in connection with complying with legal obligations or establishing, exercising or defending rights or claims (e.g., for court and arbitration proceedings, to regulators, law enforcement and government authorities, to attorneys and consultants).

If you are located in the European Economic Area, please note that the recipients to whom Siemens transfers or discloses your personal data may sometimes be located in countries in which the applicable legislation does not offer the same data privacy levels as the legislation in your own country. In such cases, and if this is required under the applicable legislation, Siemens shall take measures to implement adequate and appropriate guarantees to protect your personal data. In particular:

- We shall only disclose your personal data to Siemens companies in such countries if they have implemented the Siemens Binding Corporate Rules ("BCR") for protection of personal data. You can find more information about the Siemens BCR [here](#).
- We only transfer personal data to external recipients in such countries if the recipient (i) has signed EU standard contractual clauses with Siemens, (ii) has implemented the Binding Corporate Rules in their organization. You may request more information about the safeguards that have been put in place in relation to certain transfers by contacting dataprotection@siemens.com.

1.5 Retention periods

Unless indicated otherwise at the time of the collection of your personal data (e.g. within a form completed by you), we erase your personal data if the retention of that personal data is no longer necessary for the purposes for which they were collected or otherwise processed, or to comply with legal obligations (such as retention obligations under tax or commercial laws).

1.6 Your rights

The data privacy law that applies to Siemens when processing your personal data may grant you certain rights in relation to your personal data. You can learn more about these rights by contacting <mailto:dataprotection@siemens.com>.

In particular, and subject to the relevant statutory requirements, if you are located in the European Economic Area, you are entitled to:

- Obtain from Siemens confirmation as to whether or not personal data concerning you are being processed, and where that is the case, access to the personal data;
- Demand from Siemens the correction of inaccurate personal data concerning you;
- Demand from Siemens the erasure of your personal data;
- Demand from Siemens restriction of processing regarding your personal data;
- Data portability concerning personal data, which you actively provided;
- Object, on grounds relating to your particular situation, to further processing of personal data concerning you.

1.7 Threat and Risk Assessment

The Customer is responsible to ensure that the mobile device is under his immediate possession always.

1.8 Contact

Our Data Privacy Organization provides support with all questions relating to data privacy. You may also submit complaints against our Data Privacy Organization and assert the rights set out in this Data Privacy Notice.

You can contact our Data Privacy Organization at dataprotection@siemens.com.

Our Data Privacy Organization will always use reasonable efforts to address and settle any requests or complaints you bring to its attention. Besides contacting the Data Privacy Organization, you always have the right to approach the competent data protection authority with your request or complaint.

1.9 Usage by children

This app is not intended for children under the age of 13. We will not knowingly collect personal data from children under the age of 13 without prior parental consent if required by applicable law. We will only use or disclose personal data about a child to the extent permitted by law, to seek parental consent or to protect a child.

1.10 Data security

To protect your personal data against accidental or unlawful destruction, loss, use, or alteration and against unauthorized disclosure or access, we use adequate physical, technical and organizational security measures.

1.11 Only for US residents

The following more detailed information applies to US residents:

Do Not Track

Our Online Offerings do not recognize or respond to "Do Not Track" browser signals. For more information on "Do Not Track", please visit your browser's support page.

Your rights in certain US states

Depending on the US state in which you reside, you may have special rights with respect to your personal data. You can find additional information [here](#).

2 SIMATIC Unified AR

"SIMATIC Unified Augmented Reality" expands on-site reality by making relevant information available at all times.

The connection to information is implemented via barcodes¹. Information is displayed in "screens" in the immediate vicinity of the barcodes used.


A compilation of screens is called a "composition".

You have the possibility to link screens to systems. Systems include, for example:

- configured screens of IEDs and HMI devices;
- UIs of Edge and Mindsphere apps;
- a running WinCC Unified Runtime;
- WinCC V8, or
- any HTML pages (on the intranet or Internet).

2.1 Configuring barcodes

- Use any barcode in your environment to set up your composition or screen.
- If the "Allow new" slider is enabled, you can configure a new composition based on an existing barcode.
- If the "Allow new" slider is not enabled, the payload² of the barcode can be entered manually.
- The app detects barcodes that are in the field of view of the camera of your mobile device.

To scan barcodes, press and hold .

- If a barcode is recognized and available for configuration, a "New configuration" tile appears.
- If a barcode has already been linked to a composition without configuring screens and systems, an "Empty configuration" tile appears.
- Tapping on a tile takes you to the composition menu.

¹ Includes all usable opto-electronically detectable fonts.

² The term payload describes the data or the "content" of the barcode, which is visualized by means of a barcode.


2.2 The Composition menu

On the left-hand side, the compositions are displayed by name. Compositions can also be added using the "+" sign in the upper left corner. The following parameters of a composition are available:

- Name (give your composition a name)
- Barcode payload (displays the contents of the barcode)
- Screens (configure your screen)

When an existing barcode is scanned, its payload is automatically specified. Conversely, you can generate your own barcode by typing any string into the input line.

"Share barcode" allows you to share, save or print the barcode.

The gear wheel icon  in the title bar of a screen takes you from the AR view to the composition menu at any time.

2.3 The Screen menu

In this menu the *Screens are linked to systems*, and *title* and *size* of the screen, as well as its *Position in the 3D space* are adapted. The following parameters are available:

- **System** (type of system): Web page, Edge device, WinCC Unified Runtime, WinCC V8
- **Screen** or **Application**: If it is an Edge device, the corresponding Edge application is selected instead of the screen.
- **Title**: Name of the screen to be displayed.
- **Title bar**: Display the system name above the screen.
- **Width**: Width of the screen between 400 and 4096 [px].
- **Height**: Screen height between 400 and 4096 [px].
- **X, Y, Z**: Offset of the screen in X, Y and Z directions [cm].

Repeat the configuration for the desired number of barcodes or number of linked screens.

Comment

Make sure to move the screens around in the area so that they don't overlap and everything is visible³.

³ Will be adapted in the new version.

2.4 The System menu

- Under "Path," tap "System" to configure a system. You are taken to the System menu.
- Press "Add system" and specify the type and corresponding system URL.

2.4.1 Certificates

- To test the connection to the specified system, click "Test connection". The certificate of the respective system is checked.
- The app informs you if it is an untrusted certificate. More information is displayed.
- At the top left, tap "Cancel" if you don't trust the certificate. The certificate is stored as untrusted⁴.
- Tap "Trust" in the upper right corner to accept and save the certificate as trustworthy.

2.4.2 System authentication

When connecting to systems, with the exception of web pages, access data must be entered once. These consist of a *user name* and *password*. Access data is saved until you delete it manually.

Once a system is configured, it appears in the system menu for quick selection.


- To change or delete a system, navigate to the system menu.
- In the list, find the system whose data you want to delete or edit.
- To edit your data, tap "change" on the desired system.
- To delete a system, press and hold the selected system in the list or swipe to the left:
 - Option 1: Swipe briefly to the left. The "Delete" icon appears, select it to delete.
 - Option 2: Swipe all the way to the left to delete.

⁴ Certificates that have once been marked as untrusted cannot be deleted individually at this time. You can use "Reset all certificates" to reset all certificates at once.

2.4.3 Operating systems in full-screen mode

The required screen is in the field of view of the camera of your mobile device.


Tap in the middle of the screen to enter full-screen mode. Operate the system as usual.

Tap on the "Home"  icon at the top right to go to the page that is stored in the configured screen.


Tapping "Back" in the title bar will exit full-screen mode. The website is back in AR view.

2.5 Scanning barcodes

The app detects barcodes in the field of view of the camera.


Press and hold the "Scan"  button to view your composition in the area. This consists of one or more screens.

2.6 Resetting the AR view

Discard all barcodes that have already been scanned and the screens displayed: Tap the "Reload"  icon.

- Barcodes need to be re-scanned and configured.
- Access data to systems that have already been configured are retained.

2.7 Additional information and feedback

Click this icon  for more information and contact.

2.8 System requirements

- iOS 16/iPadOS 16
- Refer to this [list](#) of compatible end devices.