



Sigur software release notes

Revision dates 16/07/2026

Table of Contents

- 1. Version 1.6.8.131 (added in July 2026) 3
- 2. Contacts 16

1. **Version 1.6.8.131 (added in July 2026)**

System:

- Server protection against DoS attacks and against IP-address spoofing for amplification attacks has been implemented in accordance with the DTLSv1.2 protocol.
- Fixed a crash of the server module during face identification (IP camera) under the "Grant access only when supervised" logic.
- Fixed a server module start-up error that occurred if the database password began with the \$ character.
- Fixed an issue that could cause the server module to crash while performing an automatic database backup.
- More stable operation of the server module has been ensured when Sigur face recognition is enabled and a connection is made to the TLS port without a subsequent certificate exchange.
- Fixed a server freeze that made it impossible for client workstations to connect.
- Fixed the operation of the exit command in the AdminCLI utility.
- Fixed an error in the incorrect display of the permitted number of identifiers in the licence, which caused a false limit-exceeded trigger.

Software installation and update. During silent uninstallation with the /S flag, all graphical windows are closed correctly, and before the software is removed on the server, the server module and the database server are stopped automatically.

Client software:

- Performance has been improved and errors fixed when working on the "Cardholders" tab under conditions of continuous generation of a large number of events.
- Fixed an issue that caused the Client software to shut down when the connection to the server was restored.
- Fixed an issue whereby, when installing a client workstation on Windows, shortcuts were not created in the Start menu or on the desktop.
- Fixed an issue that caused the Client software to freeze when attempting to log in.
- Fixed an issue that caused the system to freeze while working with rules when using the "Quarantine" module.
- Fixed issues that occurred in the Client software on Linux when sending a test email during SMTP server configuration.

Controllers:

- Support has been added for the E2 Lite, E2 Pro, E4 Lite and E4 Pro controllers.
- On the "OSDP Devices" tab in the controller settings, a "Device model" column has been added that contains information about the model of the connected Sigur reader, as well as a "Settings" column for assigning functions to the

- primary and secondary operating modes of MK100 reader.
- The "Delay activating the security system (msec)" field in the controller settings has been updated: the value is now set using a slider instead of manual entry. The maximum value is 60,000 msec. The issue with incorrect saving of the security system activation time has also been resolved.
 - An archive with the current controller firmware versions has been added to the software installer. Firmware files for controllers of the current range no longer need to be downloaded from the website.
 - The stability of the connection between the controller and the server has been improved. Previously, a loss of communication could occur in certain cases. The server now polls the controllers every 30 seconds instead of every 600 seconds.
 - The controller data loading process has been refactored, which has made it possible to speed up data synchronisation and reduce the amount of RAM consumed.
 - Resolved an issue whereby the user configuration of an access point on a controller with firmware version 0.x.x was replaced with the default one when the security system activation method was changed.
 - Resolved an issue that could cause the "Failed to initiate update" error when updating the controller firmware.
 - Fixed an issue with slow data synchronisation in the controller memory when creating a new cardholder.
 - When configuring a controller, the output list for "Reader N LED3 indication line" now shows only the outputs available for that controller model.
 - Fixed an error in the operation of the encryption profile change button.
 - Fixed an issue whereby, when the standard E510 controller configuration "Two turnstiles, potential control mode" was selected, settings were applied to the "Request permit to enter"/"Request permit to exit" button parameters.
 - The "Wait time for the supervisor" timeout has been extended to apply to waiting for a second cardholder. This change is relevant for controllers with firmware version 1.24.0 and higher.

Readers:

- Support has been added for the new Sigur MK100 and MR100 v2 reader ranges.
- Support has been added for the SR100 EMB reader operating in USB PC/SC and USB HID modes.

Reader indication:

- Fixed the behaviour of the reader indication settings window in the Client software. Now, when changes are declined, indication profiles no longer disappear, and the window closes correctly on the first attempt on all tabs.
- The creation of custom indication profiles with a name beginning with "\$!" has been prohibited.
- Fixed the incorrect operation of the "Change the color" indication, in which the reader indicator flashed once instead of changing colour.
- Fixed an error in generating the attachment name for an indication profile when

sending it by email. Previously, when Cyrillic was used, the file name was displayed in encoded form in some email clients.

Mifare cards:

- Fixed read and write errors for some Mifare Classic cards in secure mode.
- Fixed an issue with converting a Mifare Plus card to SL3 using the ACR1252U reader.

Cardholders:

- Fixed an issue whereby changes to access point access rights did not take effect if there was no communication with the controller at that moment.
- On Windows, a limit has been added on the size of the image uploaded on the "Cardholders" and "Floor plans" tabs — a resolution no higher than 4K (3840 × 2160) is supported.
- Fixed an issue where the cardholder import window from an MS Excel spreadsheet closed if the selected file contained formulas.
- Fixed an error that occurred after a department was deleted if the operator had a capacity limit set for that department.
- Resolved an issue that could lead to a database access error after changing the type of a cardholder and moving to another one without saving.
- The ability to edit the Wiegand type for QR codes on the "Cardholders" tab has been removed.
- Now, when the type of an identifier issued to a cardholder is changed to QR, the format specified in the "File" – "Settings" – "PIN and QR codes" menu is used automatically. The format drop-down list is not available for editing in this case.
- A lock has been added on the format drop-down list when adding a PIN code.
- A new credential property — "Badge type" — has been added. The property is displayed in the cardholder card and is selected manually when issuing a new credential in the Client software interface. Cardholders can now be assigned cards, mobile IDs, PIN codes and QR codes. The badge type can be specified when importing cardholders from an .xls file.
- After the software update, all credentials in the W26 / W34 / W36 / W37 / W42 / W58 / W58Dec formats will be assigned the "Card" type. If necessary, the badge type can be changed manually or via the utility for bulk rewriting of the badge type by comment.
- A cardholder's QR code image can be viewed and copied on the "Cardholders" tab, as well as added to the badge printing template.
- Fixed incorrect sorting of badge templates when they are created and deleted.
- Fixed an issue whereby, when limiting a credential's validity period, the date and time previously set for another credential were automatically filled in.
- Fixed an issue with incorrect saving of the photograph in the cardholder record card.
- Fixed an error in saving changes to the credential validity period and access period during bulk editing.
- Fixed a database access error when attempting to print a cardholder's badge.
- Resolved an issue whereby, when new cardholders were created sequentially,

- the last one could be assigned the phone number of the previous one.
- Resolved an issue whereby, when a graphical badge template was copied, the data was not transferred to the new template.
- Fixed a database access error that could occur when adding a new position. Now, when attempting to create a position with a name that differs only by case, by the letters "e"/"ë", or by a trailing space, the system displays a notification that such a position already exists.
- Fixed an issue whereby the "Delete the selected item" button was active when the root department "Object" was selected.

CCTV:

- Reception of recognised license plates from the ISS (SecurOS) server on Sigur client workstations running Linux has been restored.
- Fixed an issue with the repeated logging of an access-denied event when recognising the license plate of a cardholder with a limited access period.
- HikCentral. The integration has been improved and optimised. A new version of the integration service — 1.1.0 — has been released.
- Trassir. Fixed an issue that could cause the server module to crash when attempting to pass through an access point in face identification mode.
- Macroscop. Resolved a server module crash that occurred when the integration was active.
- Domination. Fixed the incorrect display in the Sigur software of channels obtained from the Domination system.
- Fixed an issue whereby, when a cardholder's photograph was changed via the REST API, the photograph was not synchronised to the CCTV system.
- Fixed an authorisation error when opening archived video on the "Archive" tab in the Client software, which occurred when selecting an event if the operator's password contained special characters.

Monitoring:

- Fixed an issue whereby the Client software did not open after a restart if a "Security matrix" element was present in a monitoring view.
- For the "Location of cardholders" object on the "Monitoring" tab, the ability to display the cardholder's department has been added.
- On the "Monitoring" tab of the Client software, in the "Display events" modal window, the "Card presented" event filter has been removed, since this event is not displayed on this tab.
- Fixed a freeze of the Client software when an RTSP stream was unavailable on the "Monitoring" tab.
- Fixed the incorrect display of information on the "Monitoring" tab when creating a view with a text panel that uses HTML encoding together with an event list.
- Resolved an issue whereby, when the "Refresh" button on the "Monitoring" tab was clicked, the cardholder data in the "Select cardholders" window was not updated when attempting to allow passage via a floor plan.

Rules:

- A filter by access points has been added on the "Rules" tab.
- Fixed the incorrect display of zones in the settings of rules that count working time based on presence in specified zones.
- Resolved an issue with the incorrect application of a level-1 rule during bulk assignment of a rule via the "Cardholders" tab.
- Fixed issues that occurred when copying rules.
- The CODEKEY_DESC variable ("Credential comment") has been removed from the list of variables for configuring rule application conditions.

Antipassback. Resolved an issue whereby, during data synchronisation for new cardholders, the antipassback rule was applied incorrectly, which led to them being automatically added to the restriction lists regardless of the settings.

Archive. The start time of the covered period is now set as: {current date}, time From: 00:00.

Reports:

- A new "Work Discipline Report" has been added, which makes it possible to obtain basic information about cardholders' arrival and departure times. It is available starting from the free version of the software. This report can also be attached to an email when an event response is performed.
- The "Cardholders list" report now includes information about the badge type.
- The "Unused cards report" is now called the "Unused credentials report".
- In the report templates, the format of cells containing a date or time has been fixed.
- Fixed an issue with the changing of the cell background formatting in an exported report.
- Fixed incorrect filtering by cardholders when exporting a timesheet to 1C.
- "Unified time and attendance report":
 - Resolved an issue whereby the report was not generated if a cardholder's rule contained two working-time periods.
 - Fixed an error in the report whereby, when the "Show days of the week in the date column" setting was enabled, the values in the "Date" column were not displayed.
- "Duration of stay in the controlled zones":
 - Fixed the incorrect calculation of the time spent in the current zone when building the report.
 - Fixed an issue whereby rows with dates prior to the cardholder's creation were included in the report.
- "System event log":
 - Fixed the incorrect display of the start time in the report.
 - Fixed an issue whereby cardholders that the operator did not have access to were included in the report.
- "Operator action log":

- Fixed an issue whereby, when generating the "Operator action log" report, filtering by cardholders worked incorrectly. In addition, the report generation window now displays the number of rows processed from the database and the number of rows included in the final report.
- Fixed the incorrect generation of the "Operator action log" report for an operator with restricted access to departments and access points.
- Resolved an issue whereby the period for which an operator had previously requested the "Unused credentials report" could be displayed incorrectly.
- The deletion of a rule is now logged correctly in the operator action log.
- Fixed an error in the "Security event log" report whereby events for deleted security alarm zones were shown in the results.

Operators:

- The tooltip text for the "Log in by card" right has been updated.
- The "ID in IdM SUDIR" parameter is now displayed in operator rights only if the corresponding licence is available.
- Fixed an issue whereby an operator could edit the notification text on the "Cardholders" – "Notifications" tab even if the sending of application-approval notifications was disabled.
- Resolved an issue whereby it was not possible to remove a department capacity limit in the operator rights settings.
- The ability to edit the notification text on the "Cardholders" – "Notifications" tab has been removed for operators without the corresponding rights.
- Fixed an issue whereby, for system operators with restricted access to access points, point groups were not displayed in the access point filter on the "Cardholders" tab.
- Fixed an issue whereby an operator with view-only rights for cardholders could assign and remove rules.
- Fixed an issue whereby an operator without the right to edit equipment settings could change settings on the "Access points" – "Biometrics" tab.

Event Response:

- The "Select all" button now works correctly again when selecting events while creating a response based on a standard event.
- Fixed an error whereby, when configuring a response to events of the "when access is granted" and "when access is denied" types, the "Set the badge expiration date" action was not performed.
- A check of operator rights has been implemented when configuring a response that sends a report by email. Reports are now displayed in accordance with the operator's access restrictions. If the operator does not have rights to reports linked to previously created responses, events with such responses are not displayed on the "Events" tab.
- Fixed an issue that could affect the email report-sending function if the language of the client workstation differed from the language of the server.
- Fixed an error whereby, when an event with unsaved response changes was deleted, confirming the save applied the changes but the event was still deleted.

- Fixed an error in sending the work discipline report by email whereby the report file was generated in an incorrect format.

Temporary guest badges:

- Resolved an issue whereby, when a guest QR code/badge was created via the REST API, access points were not specified, which made it impossible to grant access afterwards.
- Resolved an issue whereby, when working with QR codes, additional photographs and images were processed incorrectly: the attached data was not displayed on the "Cardholders" tab or in the graphical badge template.
- Resolved an issue whereby the automatic and manual sending of an email with a guest QR code using the Sigur software was not performed if the guest had been created via the REST API.
- Fixed the absence of a value in the "Host" field when sending a QR badge by email. Previously, the field could remain empty if there was no associated application.
- Fixed an issue whereby the validity start and the actual issue date of a QR code did not match the values specified in the application.
- Fixed an error in managing the validity period of guest badges: when editing and bulk-editing cardholders, changes to the validity period and the validity-period limits were applied incorrectly, which led to a data mismatch between the "Guests" and "Cardholders" tabs. Checks of issued badges have been added and the availability of the validity-period parameters has been synchronised.
- Fixed an issue whereby, when the validity period of a guest badge was changed on the "Guests" tab, the record of its issue disappeared.
- Fixed an issue with saving the value of additional parameters when issuing a guest badge using already existing guest information.
- Fixed an issue whereby changes to the full name in the card of a guest with a QR code were not synchronised with the "Cardholders" section even after refreshing the tabs or restarting the Client software.
- Fixed the incorrect operation of the procedure for deleting the data of a selected guest.
- Fixed an error that occurred when submitting an application without specifying a document type in the application web service.
- Fixed the incorrect display of the software version in the application web service.
- Resolved an issue whereby the page with the application number and QR code did not open when an application was submitted with automatic approval via the web service.
- Resolved an issue whereby, when checking an application created in the Client software and containing several guests, the application service displayed the QR code of only the first guest, even if the document number of another participant in the application had been entered.
- Fixed an issue in the application web service whereby the notification about resending a QR code was in English.
- A validation of the data in the "Validity start" and "Validity end" fields has been added when creating a visit application.

- A new system value "Not selected" has been added for the guest document type.
- A uniqueness check of the document name when editing has been added. Spaces at the beginning and end of the name are now automatically removed and not saved.
- Fixed the incorrect display of the "Visiting" parameter value in the window with information about a guest's issued QR code. Now, if the cardholder whom the guest came to see has been dismissed or removed from the system, their full name is displayed with the "[D]" prefix.
- Fixed an issue whereby, when issuing a badge to a guest, the Email field was automatically filled in with the value example@ex.com.

Document recognition:

- Support has been added for integration with the Content AI PassportReader SDK 1.5.5 product.
- Operation with the ABBYY PassportReader SDK has been restored. For correct operation during the initial configuration, the Client software must be run as administrator.

Sigur Mobile Terminal:

- The ability to scan barcodes in the Code 128 format, as well as credentials of the "QR code" type, via the "Mobile Terminal" application has been implemented. Accordingly, a new operator right to use this function has been added to the Client software, and a new event "Code scanned: <scanned string>" is recorded in the "Archive" and in reports.
- The "Access denied. Unknown credential number." event is now recorded in the Client software when an unknown card is presented to a Sigur offline terminal.
- Fixed an error whereby, when a guest QR code was scanned in the "Mobile Terminal" application, the message "Unknown credential number" was displayed despite the presence in the system of a badge correctly issued via the application web service.

Data synchronisation:

- The functionality for synchronising data from external sources into the Sigur database has been refactored, which has made it possible to speed up the synchronisation process.
- Errors and freezes of the Client software that occurred when synchronising cardholders with an incorrect date format have been eliminated.
- Fixed an issue whereby, during data synchronisation from external sources, the same credential could be assigned to different cardholders.
- Fixed an issue whereby synchronisation from an external database was not performed if cardholders had an empty (NULL) "Credential expiration date" field.
- Fixed an issue whereby a cardholder with an empty (NULL) "Credential expiration date" field was deleted or moved to the "Dismissed cardholders" folder during synchronisation from an external database.

Active Directory:

- Fixed an issue whereby, when configuring Active Directory account blocking, the list of allowed zones was not displayed until the Client software was restarted.

Payment system:

- Fixed a freeze of the Client software during bulk addition and modification of accounts for several cardholders.
- Fixed the incorrect display of the transaction amount when receiving a notification about an account change.
- Fixed an error in saving the current-account value of a guest QR code.

Intrusion and Fire Alarm:

- Fixed an issue that caused lengthy initialisation of the Client software when there was a large number of access points and the operator had access to the "Security" tab.
- Fixed an issue whereby a restart of the server module was required for the status of a new security alarm zone to be displayed correctly.
- Display of three new events related to Sigur security alarm zones has been added: "Failed to arm the zone. Alarm line not specified", "... Reader busy" and "... Zone is already being armed". These events are available in the system reports, the "Archive" and on the "Monitoring" tab, and can also be used when configuring event responses.
- Events of Sigur controller security alarm zones are now displayed not only in the "Security event log" but also in the "Archive" and the "System event log". This change applies only to newly registered events.
- Fixed an issue whereby it was not possible to obtain the status of a Sigur security alarm zone and activate it.

Biometrics:

- Fixed an issue with generating and saving Biosmart palm-vein templates.
- Fixed the appearance of a warning about unsaved changes in the Vzor biometrics settings when there were no actual changes.
- Fixed an issue with generating a Biosmart Quasar biometric template that occurred when Cyrillic was used in the OS user name.

Integration with Suprema face recognition terminals:

- The performance and stability of the integration service have been optimised.
- Support has been implemented for the integration to work with Sigur servers running Debian Linux and RHEL.
- Support for the PostgreSQL DBMS as an external ACS database has been added.
- Interaction with Suprema devices over OSDP has been tested.
- Fixed an issue that caused the Client software to freeze and errors to appear in

the logs after enabling the Suprema integration in the "File" – "Settings" – "Biometrics" menu.

- Resolved an issue whereby the supremaservice process did not terminate and the Client software froze after the integration was disabled on Linux.
- Fixed an issue whereby the Suprema integration continued to work after the licence had expired.
- Fixed the incorrect display of the "Credential code type for generation" field in the "File" – "Settings" – "Biometrics" – "Suprema" menu.
- Fixed an issue whereby biometric templates were not loaded into Suprema terminals when Biosmart Quasar templates were present in the system.
- Resolved an issue that could cause the server module to crash when attempting to add a fingerprint using Suprema devices.
- Fixed an issue with synchronising cards to Suprema terminals when the validity-period limit was removed for several cardholders at the same time.

Integration with Hikvision face recognition terminals:

- The integration has been optimised – the load on the server has been reduced and data synchronisation has been sped up.
- Fixed a data synchronisation error with Hikvision terminals when using version 1.5 of the integration service on Linux with the PostgreSQL DBMS.

Integration with BAS-IP:

- Fixed an error whereby cardholder information was not synchronised with the memory of the intercoms.
- Fixed an issue with synchronising credentials of the "Mobile ID" type with the memory of the intercoms.

Integration with the Keyguard key cabinet:

- Eliminated the persistent prompt to save changes when selecting access rules in the Client software, which appeared even when there were no changes.
- Fixed the incorrect display of the list of key access rules when assigning rights to cardholders.

Integration with Dormakaba. Fixed an issue whereby the list of access points and passage events was not synchronised from the Matrix software.

WebDel integration protocol. Fixed an error whereby, when access was denied by a decision of an external system, the event "Access denied. The rule does not permit passage" was generated.

REST API:

- New event types returned in response to the GET /api/v1/events, GET /api/v1/events/types and GET /api/v1/events/parsed requests have been added:

- "Controller power state change" (DC_STATUS).
 - "Controller battery state change" (BATTERY_STATUS).
 - "Failed to change access point mode" (AP_MODE_DENY).
- The VOLTAGE_STATUS event type is no longer used.
- The armingMethod attribute has been added to the "Security alarm zone status" event (ALARM_LINE_STATUS). The attribute is returned in the GET /api/v1/events/parsed request if the zone was armed using a Sigur MK100 reader.
- New reasons for some event types returned in response to the GET /api/v1/events/parsed request have been added:
 - For the PASS_DENY event:
 - "Access period expired or not started" ("Access denied. The access period has not started or has already ended");
 - "Waiting for confirmation of access point mode change" ("Access denied. Waiting for confirmation of the access point mode change");
 - For the WAITING_FOR_RULE_STAGE event:
 - "Waiting for second access object" ("Waiting for a second access object for access");
 - "Waiting for confirmation of access point mode change" ("Waiting for confirmation of the access point mode change");
 - For the MNG_STATE_CHANGED event:
 - "PIN", "PIN AND PASS" (change of the access point mode using a PIN code or a PIN code confirmed by a credential).
- New event types returned in response to the GET /api/v1/events, GET /api/v1/events/types and GET /api/v1/events/parsed requests have been added:
 - "Failed to arm the zone" (ALARM_LINE_DENY);
 - "Security alarm zone status event" (ALARM_LINE_STATUS).
- For the WAITING_FOR_RULE_STAGE event, a new reason "Waiting for confirmation of zone arming" has been added. The alarmZoneId attribute has been added to the data object, and the alarmZone object to the additionalData object.
- New endpoints have been added for working with guest cards and QR codes, for managing the issuance of guest cards, and for managing cardholders' QR and PIN codes.
- A tabid field (department number) has been added to the parameters of the departments object, also available when creating and editing departments.
- The ability to add, change and delete the MFUID of cards has been added.
- The Employees and Official Vehicles group requests have been updated:
 - the cardholder's access period and the verification PIN code can now be specified when creating a cardholder, and changed and retrieved via the REST API (the accessStartTime, accessEndTime and verificationPin attributes have been added);

- an identifiers object containing all the identifiers of the cardholder has been added to the bodies of some requests and responses;
- the set of filters has been expanded: the IN, NEQ, IS_NULL, IS_NOT_NULL and CONTAINS operators are now supported for filtering by additional parameters in the GET /api/v1/employees request.
- The logic for working with cards that have the guestApplicable=true attribute has been changed.
- The GET api/v1/cards and GET api/v1/cards/{id} requests now return only credentials of the "Card" type. To view the mobile IDs, QR codes and PIN codes of cardholders, use the GET /api/v1/employees and GET /api/v1/employees/{id} requests.
- The processing of the GET /api/v1/events/parsed and GET /api/v1/events requests when using time-based filtering has been optimised.
- Fixed errors that occurred when generating a guest QR code using the PUT /api/v1/guests/{id}/QR request.
- Fixed an issue whereby the response to the GET /api/v1/guests request for guests of the "QR" type contained a guestCardId attribute, by which information could be obtained via the GET /api/v1/guestcards/{id} request.
- Fixed the incorrect representation of the value and formattedValue fields in the response to the GET api/v1/guestcards/{id} request.
- Fixed an issue whereby default rules could be deleted using the DELETE /api/v1/accessrules/{id} request.
- Resolved an issue with the incorrect processing of the GET /api/v1/bindings/employees-guestcards request when using the includeFields, excludeFields, limit and offset parameters.
- Fixed an HTTP 500 error when executing the GET /api/v1/guestcards request with the value and sortBy parameters. Sorting by the assigned and formattedValue fields is not supported for this request.
- Fixed an HTTP 500 error when attempting to delete the value of a mandatory additional parameter using the PUT /api/v1/employees/{id} request.
- Fixed the validation of card values when creating them via the REST API. It is now impossible to create a card or QR code with a zero code.
- Resolved an event-processing issue whereby the GET /api/v1/events/parsed request could return an empty response.
- Fixed an HTTP 500 error when executing the GET /api/v1/events request if the ACS server was running Linux.
- Fixed an issue whereby the GET /api/v1/employees request returned all cardholders if a non-existent additional parameter was used in the search. The server now returns the HTTP 422 status in such cases.
- Fixed an issue whereby filtering by accessObjectId did not work in the GET /api/v1/events/parsed request when using the PostgreSQL DBMS.
- The GET /api/v1/employees request executed on behalf of an operator with full restriction of access to departments now returns a 200 OK response and an empty result.
- Fixed the operation of the filter by tabid in the GET /api/v1/employees request.

Other bug fixes and system optimisation:

- Fixed an issue whereby the "Server Administration" software did not start.

- Other causes that could lead to system freezes and reduced performance have been eliminated.
- Fixed an issue that could cause the "Device configuration" – "Set up IP devices" tab in the "Server Administration" software to freeze.
- Fixed an issue with the slow operation of the "Cardholders" tab when using the Biosmart integration.
- Fixed errors related to the untimely updating of information about the licence loaded into the Client software.
- The help description for the "Alcohol testing" parameter has been clarified in the settings of breathalysers connected to Sigur controllers via the Wiegand interface.

2. **Contacts**

For any inquiries or assistance, please contact us using the provided information.

Website: www.sigur.com

General Inquiries: info@sigur.com

Technical Support: support@sigur.com