



phion live assist - the phion remote support concept



➤ White Paper

phion live assist the phion remote support access concept	3
How does it work?	4
Where does that identification string come from?	5
How do I get going?	6
Is it really secure?	6
How do we protect your privacy?	7

the phion remote support access concept

Complex enterprise IT environments need powerful security products to protect them. Once deployed the security infrastructure becomes itself a critical element within the overall infrastructure. Thus when something goes wrong and the in-house team cannot pinpoint the cause adequately then quick and competent assistance from the outside be it from a service partner or the vendor itself is needed.

The typical safeguard against failure of a particular critical security device is a redundant setup. But equipment malfunctions are not simply restricted to device failure but sometimes occur in the course of a software update, a seemingly innocuous configuration change, or a spurious change in the environment, e.g. bursts of traffic or a novel particular traffic flow pattern. In the latter case redundancies will not help as also any intervening backup system will show a similar behaviour as the previously failing device - provided hardware, software and configuration state are identical - as is normally the case.

The most cost-efficient and effective way to support an ailing customer installation is via remote access to the affected security device using the native management application.

The traditional way of problem reporting to the support organisation often involves various iterations of queries for additional information until the actual root cause can be determined. Customer dissatisfaction is inevitable if the condition cannot be resolved quickly. At the supporting end higher costs are incurred because of the repeated involvement of various support team members over a longer period of time.

The downside to this is that remote network access and knowledge of administrative accounts and their access credential is typically required by the remote support personnel. For many enterprise customers this is not reconcilable with their security policies.

Granting exceptions is a cumbersome and lengthy procedure as it is commonly subject to approval by a corporate security officer.

Typical scenarios where competent and quick remote support access is needed:

- Infrequent malfunctions that are hard to reproduce outside the actual productive environment
- Recurring malfunctions that only originate under certain operating conditions
- Internal resources with limited know-how and/or capacities
- SLA requirements calling for short reaction times
- Hard to reach remote locations

Typical remote support approaches:

- Fully outsourced operations! (console operations/assistance)
- VPN access to systems (requires external connectivity!, fixed address etc., requires password to be passed on)
- SSH or dial-up access to console
- Online meeting tools such as Webex, Adobe Acrobat Connect Pro, gotomeeting, etc. (external third party)
- Site visit (too expensive, overly long reaction times)



In order to facilitate expedite remote assistance when needed phion offers its own remote support tool "phion live assist". It allows a customer to share their management application with a support engineer. Furthermore file exchange from and to the customers workstation is facilitated. This way larger log files or hotfixes may be exchanged. Note that the file transfer is implemented in an interactive manner rather than accessing the file system directly. The receiver is always asked if he wants to accept the sent file and decides where to place and how to name it. In addition live assist allows chat sessions between the attending parties. Other than in the case of direct access to the gateways here the customer can observe all actions carried out by the supporting engineer in real time. Live assist provides many of the features well known from popular online meeting tools but avoids all downsides that result from bringing in an additional service provider:

1. It is free to use, i.e. you do not have to sign up with any of the meeting tool service providers or pay them money for hosting a session.
2. It warrants privacy - it is all between you and us and you stay in control, always.
3. It is as secure as our VPN technology - as you trust our security products you may also trust our remote support concept.
4. It is limited to the management application phion.a only, you share your view on phion.a with us, we don't need to know or have any access credentials.

How does it work?

When implementing phion live assist we took special care that only relevant information is shared and that the party requiring assistance always stays in charge.

Therefore a session can solely be initiated by this party. But in order to activate live assist a few other prerequisites are needed:

1. An identification string that is shared by both the user and the supporter is required to establish the actual remote access connection.
2. Someone waiting for an incoming session request for the particular shared secret. This necessitates a prior registration at the rendezvous-server that will terminate the incoming request with exactly that identification string.

Someone needing assistance that will now use the shared identification string - much like a shared secret - to establish the actual live assist session that the supporting party is already waiting for.

Where does that identification string come from?

The identification string is commonly referred to as support ticket identification number or ID.

The ticket ID may either be a number referring to an actual support case or it is an arbitrary alphanumeric string that can be generated through a Myphion interface by any appropriately authorised Myphion users.

In the case of actual support tickets the ticket is generated by phion support staff and the user requesting assistance typically is a channel partner servicing a customer system or a direct support customer.

Ticket creation through Myphion can be used by a channel partner or anyone appropriately authorised to provide support through the live assist mechanism.

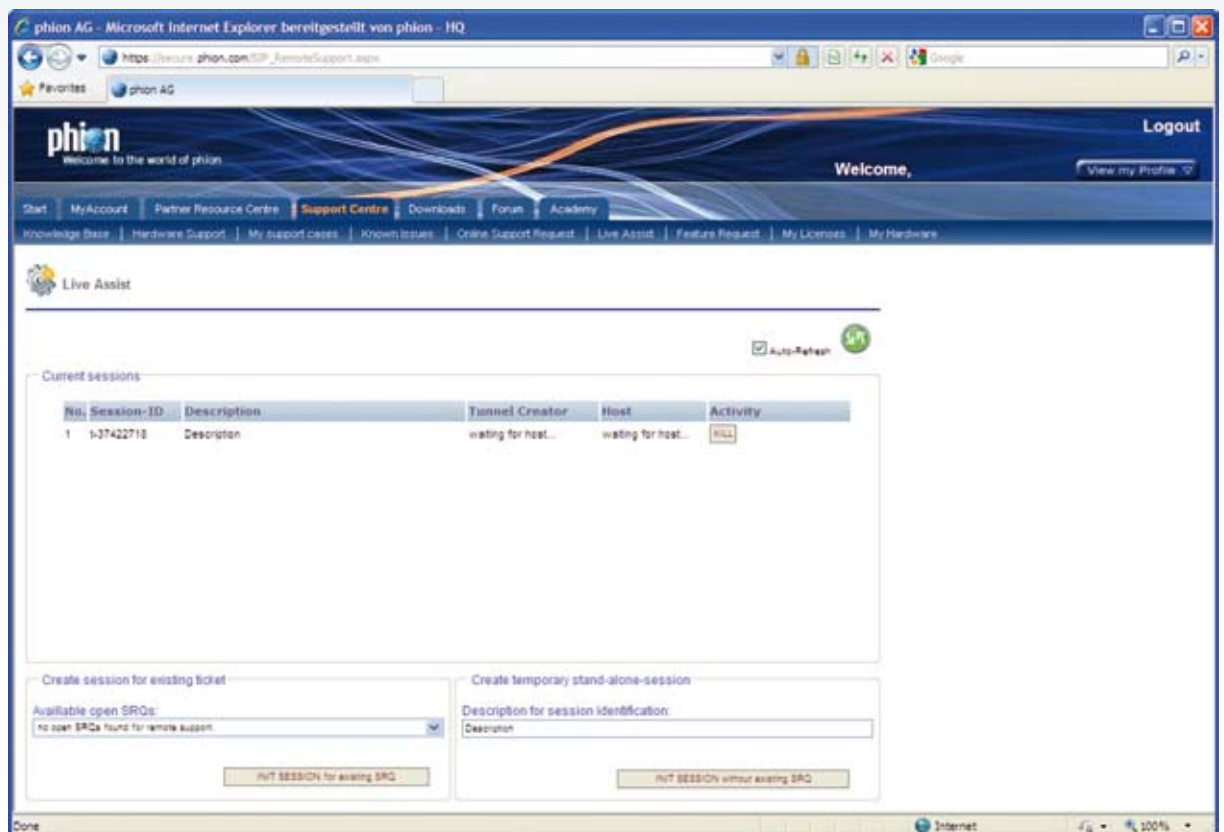


Figure 1 - Myphion web interface that allows ticket number creation and session slot initiation at the rendezvous server. In addition any existing sessions which the user is entitled to join would be displayed.

How do I get going?

Once a session slot has been created at the rendezvous server hosted and the required identification number has been shared the person requiring assistance may actually start the session.

Here you simply start up your phion.a (starting from 4.2.7 on) and click on the support/live assist button in the tool bar.

This brings up a dialog where you may insert the assigned identification number and your name alongside a range of security and privacy relevant options. Once you hit the OK button an outbound SSL encrypted connection will be launched that connects to <https://mysupport.phion.com>. If your workstation is located behind an Internet facing web proxy you will have to specify address and port as well as user and password - if required - first in order to establish the connection successfully.

The outbound connection terminates at the Myphion.com rendezvous server where it is registered and associated with the session slot that has already been created for that particular identification number. Through the rendezvous server access to phion.a running on the user's workstation can be gained.

Session establishment only actually happens when an appropriately authorised phion support engineer or assigned phion partner has informed the system that he or she is waiting to handle the incoming session request. This way the user is not unintentionally unattended nor will he ever be forced to share his application unwittingly.



Figure 2 - Illustration of the various parties that may be involved in a live assist session. The most common case being a phion partner being attended by phion staff out of a phion support center. In this the partner will probably have managed to get access to the customer's device by other means. A partner and a customer may independently of a support case always use the secure rendezvous server to have a live assist session between them. In the case of direct support contracts a customer and phion support staff may have a direct live assist session.

Is it really secure?

Yes, especially since the connection can only be initiated by the customer. The remote end is uniquely identified via a x.509 digital certificate which on first connect is shown to the customer for approval. This validation protects against man-in-the-middle attacks and connection hijacking. Any established connection is then encrypted using the AES algorithm with 256 bit keys.

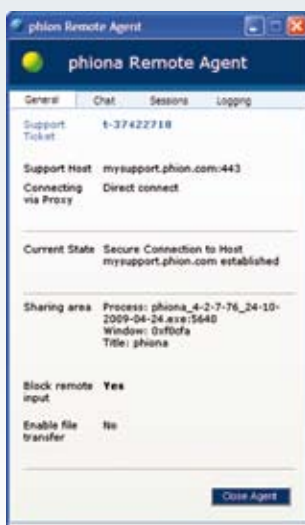
How much control you hand over to the support engineer is entirely at your discretion when you initiate the connection. The following controls are available :

- Allow input from the remote end, OFF by default
- Support file transfer, OFF by default

What is going on is always appropriately visualised through the phion.a Remote Agent window which appears after a session request was started.

It displays both security policy settings as well as the connection state with respect to ongoing remote access connections.

Note also that even when you have consented to the file transfer option this does not mean that data may just be uploaded to your workstation. An incoming file will bring up a dialog which you may use to save the file somewhere or alternatively refuse to accept it.



How do we protect your privacy?

We do not require you to share the complete desktop but rather the management application only. Sharing requires an identification number which may be obtained from us after having opened a support case. The extent to which you wish to grant access to your workplace is controlled by policy settings you select prior to starting the session request.

The following options are available

1. Screen application protection, ON by default disables the window bar
2. Extent of allowed view, full phion.a (DEFAULT) or just box or MC access without any menu or tool bars

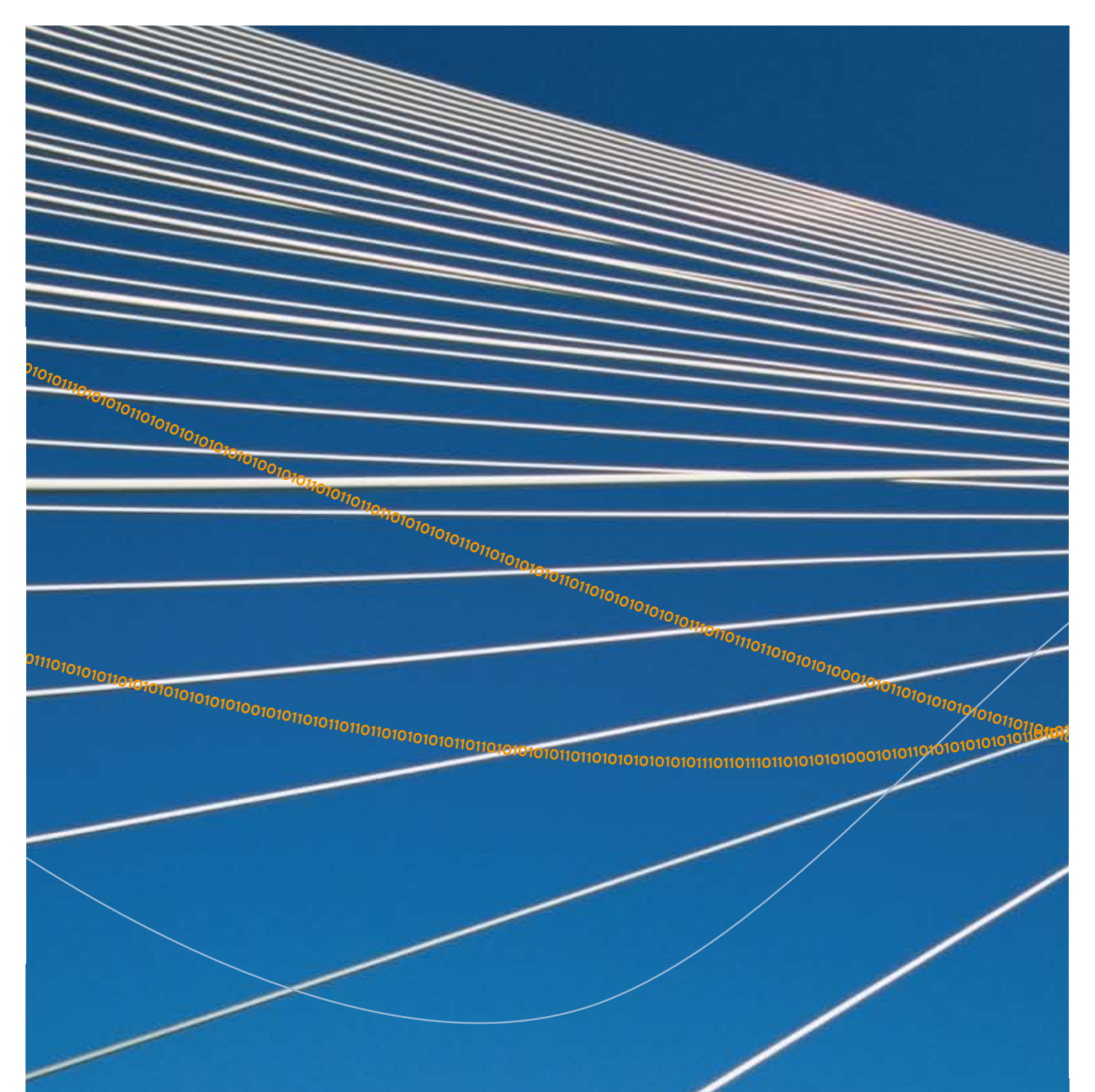
Apart from limiting the shared view to the bare minimum actually needed to get the job done it is also important to know who else will actually get access to that view.

The overall policy we adopt is as follows:

- A support call is opened by a partner's employee on behalf of a customer or by a customer's employee provided the customer has a direct support contract with phion.
- The ticket with its identification number is assigned to the person having reported the problem and a member from the phion support team. Together with this assignment also the organisation the person belongs to is associated with the support case.
- Myphion users with appropriate authorization will see any established sessions that have an association with anyone from their organisation within Myphion and may also join them. This means that team-based support may be provided without everyone having to be in the same location. The entry point to join such a session is the Support Centre tab inside the Myphion portal, cf. Figure 1
- phion support staff may see and join any session.

In addition appropriately authorised users may also create a temporary session slot so to have a private session that does not involve the phion support team but still is relayed through our trustworthy backend infrastructure. This facility is intended to enable partners to provide better remote support and to provide an easy means to help a customer with test installations.

Note that the web interface shown in Fig. 1 is still being worked on. Additional features such as chat and ability to upload files are still missing from it. They are presently restricted to phion staff.



www.phion.com



phion AG
Eduard-Bodem-Gasse 1
6020 Innsbruck
Austria

Fon: +43 (0)508 100
Fax: +43 (0)508 100 20

office@phion.com
www.phion.com