GARRISON

Deploying Garrison ULTRA®

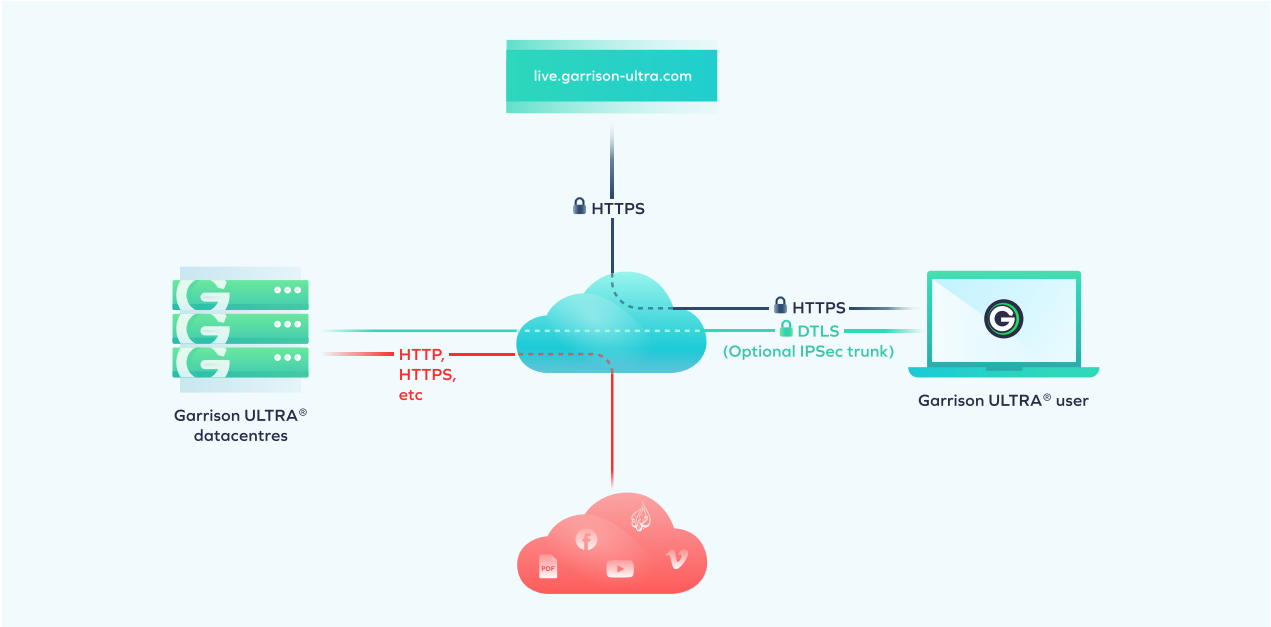
As simple as signing up and getting going

Deploying Garrison ULTRA® – for an initial Proof of Concept, or for production use – is very straightforward, but you may wish to optimise your experience by considering integration with SAML and with your proxy or other Secure Web Gateway. Additionally you may need to consider network traffic options, user activity logging, and capacity management.

Traffic routing

Garrison ULTRA® is delivered to your Chrome or Edge browser (support for further browsers may be added in the future). Two data streams are generated by the browser:

- HTTPS traffic to https://live.garrison-ultra.com
- WebRTC (DTLS) traffic to one of our Garrison ULTRA® data centres. IP addresses for our data centres are listed on the Garrison ULTRA® support portal.



We can support secure trunks to our data centres using IPSec. Contact us if you would like to understand more about this option.

Deploying Garrison ULTRA®

Capacity management

What is a Browsing Session?

With Garrison ULTRA®, you purchase a number of concurrent browsing sessions for your organisation. A browsing session begins when a user connects, or reconnects, to Garrison ULTRA® and continues while the user actively engages with the service by scrolling, clicking or typing.

Suspended Sessions

If a user stops actively engaging, their session will time out and enter a "suspended" state. From a suspended state, reconnecting involves a single click, and is typically instantaneous. Suspended sessions do not count towards your limit of concurrent browsing sessions, however if the limit of active browsing sessions is reached while a session is suspended, the suspended user will not be able to reconnect due to a lack of capacity.

Concurrent session limits

If you reach the limit of available sessions, new users trying to connect to Garrison ULTRA® will receive a message informing them that there is no available capacity. They must wait for capacity to become available to reconnect.

SAML or license key?

There are two options for your users to authenticate to the Garrison ULTRA® service.

Licence Key

The simplest option is an organisational license key, which can be used in one of two ways:

- Typed into the web page at **live.garrison-ultra.com**
- Supplied as a parameter to the URL: **https://live.garrison-ultra.com/?k=<license-key>**

The license key only needs to be supplied the first time a user connects to Garrison ULTRA®.

With this option, Garrison ULTRA® will not know the individual identity of your user – only the organisation they are connecting from.

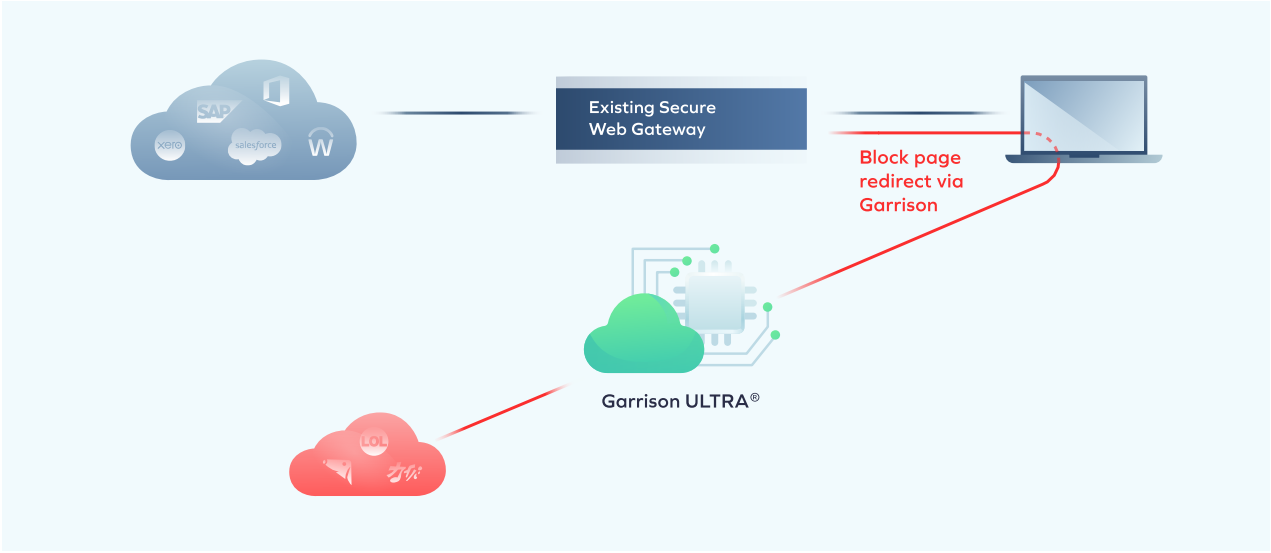
SAML-based SSO Authentication

Set up SAML-based SSO authentication for your users by providing Garrison ULTRA® with the metadata for your SAML-compliant IdP. With SAML based authentication, Garrison ULTRA® will know the individual identity of the user and be able to include this information in browsing logs (see below)*. Users can identify their organisation the first time they connect either by manually entering their email address, or using the license key approach (each organisation will continue to be allocated a license key even if SAML authentication is used).

Deploying Garrison ULTRA®

Proxy redirection

Users can connect to Garrison ULTRA® at any time by visiting **https://live.garrison-ultra.com/**. But in addition, you may wish to set up proxy redirection to provide users with a more seamless workflow.



With proxy redirection, you modify the block page served up from your existing proxy (or other Secure Web Gateway) so that users are automatically redirected to visit the requested site using Garrison ULTRA®. For example, if the user tries to visit **https://dubiouslink.com/**, the user can be redirected to **https://live.garrison-ultra.com/?url=https://dubiouslink.com/** – i.e. providing the original URL as a parameter. The redirect can either be immediate – or you can use this as an opportunity for cybersecurity training and awareness by including a message such as "This site is considered to be high risk from a security perspective and must be visited using a special security tool called Garrison. To proceed, click here".

If use of Garrison ULTRA® is being restricted to particular user groups, many proxies or SWGs can support serving different block pages for different user groups.

Redirection Strategies

Many different strategies can be used for proxy redirection depending on your particular risk profile and preferences. Examples include:

- Redirecting sites that are currently blocked, in order to reduce user frustration and helpdesk calls
- Redirecting URL categories considered to be risky, together with uncategorised URLs
- Using dynamic URL risk scores based on threat intelligence to redirect high risk URLs
- Maintaining an allow-list of URLs that can be accessed natively, and redirecting all other URLs

Deploying Garrison ULTRA®

Email Link Rewriting

For some customers, the priority is addressing the problem of links in phishing emails – links that could lead to ransomware or other malicious attacks.

Just as with proxy-based redirection, some 3rd party email gateway technology provides facilities for link rewriting in inbound external emails.

Where this is supported, links can be redirected to Garrison ULTRA® exactly as with proxy redirection – rewriting **http://dubiouslink.com/** to **https://live.garrison-ultra.com/?url=http://dubiouslink.com/**

Note that implementing this link rewriting approach will be dependent on the facilities provided by your mail processing gateway.

Browsing logs

Garrison can provide logs of the websites visited by your Garrison ULTRA® users. If SAML authentication is enabled, these logs will include the identity of the user*.

*NOTE: During the Beta phase of Garrison ULTRA®, setting up SAML and obtaining browsing logs will involve interacting with the Garrison Customer Success team. An administrative portal will be introduced in the future.

Email info@garrison.com
UK Telephone +44 (0) 203 890 4504
US Telephone +1 (646) 690-8824

CD00000590v2.0 – December 2021