[V8] FAQ: Should you use the default Ahsay dummy / self-sign certificate for your business?

Article ID: 8037
Reviewed: 2019-03-27

Product Version:
Ahsay Software: 8.1 to 8.x
OS: All platforms

Description

Should you use the default Ahsay dummy / self-sign certificate for your business?

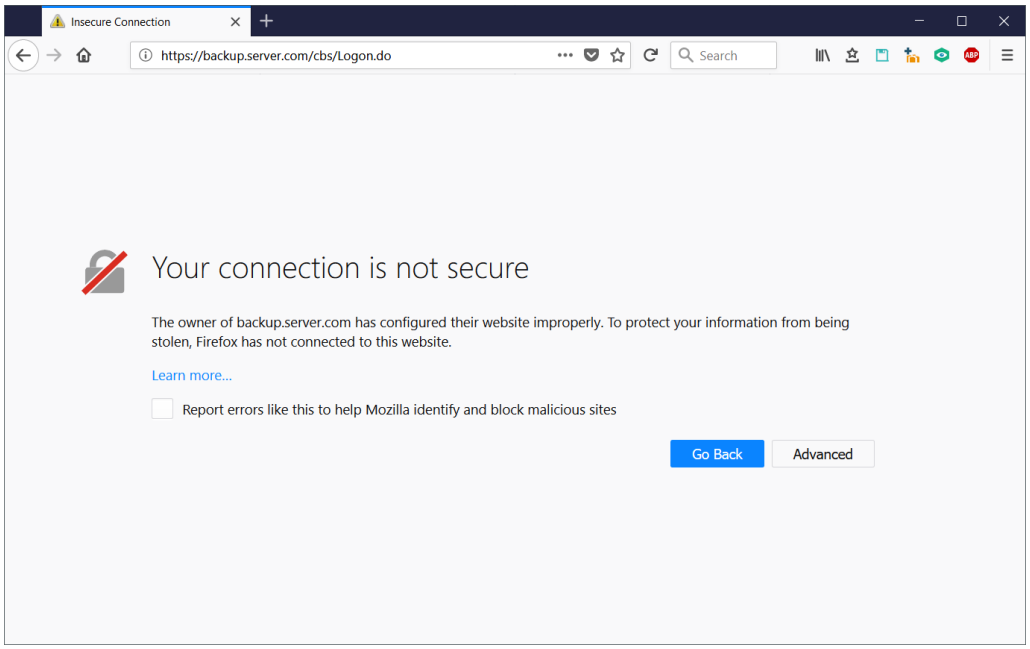
Contents

The Ahsay dummy / self-sign certificate, which is bundled with every AhsayCBS installation by default, is a handy tool to have, but using it for a production backup server could be a big mistake.

Here's when it makes sense and when it doesn't.

For a public facing backup server
For any public-facing backup server (WAN environment), it is never a good idea to deploy your AhsayCBS with the default Ahsay dummy / self-sign certificate. That is, even if you have never suffer a security / cryptographic attack of any sorts, you must put forth a very trustworthy front for your customers, as the slightest security misstep could be catastrophic to your company's image.

Does this look like a trustworthy website to you?



While the default Ahsay dummy / self-sign certificate also encrypt customers' data and other account credentials, most browsers such as Google Chrome and Mozilla Firefox will display a security alert because the default Ahsay dummy / self-sign certificate was not verified by a trusted Certificate Authority.

The security warnings associated with the default Ahsay dummy / self-sign certificate may drive away potential customers with fear that the website does not secure their credentials and data. Both brand reputation and customer trust are damaged.

For an internal facing backup server
For internal backup server (LAN environment), the default Ahsay dummy / self-sign certificate should only be used on a temporarily base (e.g. proof of concept phase), or for testing purposes.

Many organizations advise internal users to simply ignore the warnings since they know the internal web console is safe, but this could encourage dangerous public browsing behavior. Internal users accustomed to ignoring warnings on internal sites may be inclined to ignore warnings on public sites as well, leaving them, and your organization, vulnerable to malware and other threats (e.g. open to man-in-the-middle attacks).

To conclude, the simple fact is, the default Ahsay dummy / self-sign certificate should only be used for temporarily internal LAN-only services, or for testing purposes.

For any other setup, it is strongly recommended to install a trusted SSL certificate for your backup service.

Note:
For instruction on how to install a trusted SSL certificate for your AhsayCBS server, refer to the instruction provided in the AhsayCBS Administrator's Guide. Click Here for the list of Ahsay trusted CA. Alternatively, you can also let our professional service team to help you with the SSL certificate CSR generation and SSL certificate installation. Click Here to visit the Ahsay Shopping Centre for subscription.

Please note that it is not Ahsay System's obligation to renew a dummy certificate since the default Ahsay dummy / self-sign certificate is only intended for functionality testing purposes.

Keywords

ahsay, self, sign, selfsign, self-sign, cert, certificate, ca, dummy, default, security