uSync Publish Security Hardening.

When using uSync.Publisher, you can use it out of the box, and it will sign all communication between servers ensuring only secure and authorised communication is allowed. However, you may wish to harden your uSync.Publish Installation. The following will help you when hardening your setup:

Use https

You should use an https connection between servers to ensure that any communication is encrypted and secured

Use a secure AppId/AppKey

When you set up publisher it will generate an AppId/AppKey pair, these can be any string, but you should make sure you do not share these key and use values that are hard to guess/crack via brute force.

Secure “/umbraco/uSyncReceive” route

All incoming requests will be handled by the uSyncReceiveApi controller which answers on a route of /umbraco/uSyncReceive/uSyncReceiveApi/ you could choose to secure this route via IP address or another network setting to reduce the number of clients that can connect to your server.

For example to restrict to an internal network and localhost you might add this to your sites web.config file.

```
<location path="umbraco/uSyncReceive">
 <system.webServer>
 <security>
  <ipSecurity allowUnlisted="false">
   <add allowed="true" ipAddress="192.168.0.1" subnetMask="255.255.255.0"/>
   <add allowed="true" ipAddress="127.0.0.1" subnetMask="255.255.255.0"/>
  </ipSecurity>
 </security>
 </system.webServer>
</location>
```