Microsoft

IS Crypto is a free tool that gives administrators the ability to enable or disable protocols

IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2008, 2012, 2016 and 2019. It also lets you reorder SSL/TLS cipher suites offered by IIS, change advanced settings, implement Best Practices with a single click, create custom templates and test your website.

Features

- Single click to secure your website using Best Practices
- Backup the registry before making any updates
- Change advanced registry settings
- Built in Best Practices, PCI 3.2, Strict and FIPS 140-2 templates
- Create custom templates that can be saved and run on multiple servers
- Revert back to the original server's default settings
- Stop DROWN, logjam, FREAK, POODLE and BEAST attacks
- Enable TLS 1.1 and 1.2
- Enable forward secrecy
- Reorder cipher suites
- Disable weak protocols and ciphers such as SSL 2.0, 3.0, MD5 and 3DES
- Site Scanner to test your configuration
- Command line version

What Does IIS Crypto Do?

IIS Crypto updates the registry using the same settings from this article by Microsoft. It also updates the cipher suite order in the same way that the Group Policy Editor (gpedit.msc) does. Additionally IIS Crypto lets your create custom templates that can be saved for use on multiple servers. The command line version contains the same built-in templates as the GUI version and can also be used with your own custom templates. IIS Crypto has been tested on Windows Server 2008, 2008 R2 and 2012, 2012 R2, 2016 and 2019.

IIS Crypto requires administrator privileges. If you are running under a non-administrator account, the GUI version will prompt for elevated permissions. The command line version must be run from a command line that already has elevated permissions.

Downloads

IIS Crypto is offered in both a GUI and a command line version. Click here to choose your version and download.

Custom Templates

IIS Crypto allows you to create your own custom templates which can be saved and then executed on multiple servers. To create your own template, select all of the settings for your configuration. Click on the Templates button and give your template a name, author and description if desired. Then click on the Save button to save your template to disk. Copy your template to another server, run IIS Crypto and click on the Open button to load your template. You can also use it from the command line version of IIS Crypto.

The template format has been simplified in IIS Crypto 3.0. Old templates are automatically upgraded when loaded, however, if you save a new template it will only open in IIS Crypto 3.0 and later.

Load the Best Practices template before you start customizing your own template to ensure your template is setup securely. If your template is in the same folder as IIS Crypto it will show up automatically in the drop down box without having to click the Open button first.

Command Line Help

The following are the switches for the command line version of IIS Crypto. All parameters are optional.

Switch	Option	Description
/backup	<filename>	Specify a file to backup the current registry settings too.
/template	default	This template restores the server to the default settings.
	best	This template sets your server to use the best practices for TLS. It aims to be compatible with as many browsers as possible while disabling weak protocols and cipher suites.
	pci32	This template is used to make your server PCI 3.2 compliant. It will disable TLS 1.0 and 1.1 which may break client connections to your website. Please make sure that RDP will continue to function as Windows 2008 R2 requires an update. See our FAQ for more information.
	strict	This template sets your server to use the strictest settings possible. It will disable TLS 1.0 and 1.1 and all non forward secrecy cipher suites which may break client connections to your website. Please make sure that RDP will continue to function as Windows 2008 R2 requires an update. See our FAQ for more information.
	fips140	This template makes your server FIPS 140-2 compliant. It is similar to the Best Practices template, however, it is not as secure as Best Practices because some of the weaker cipher suites are enabled.
	<filename>	Specify the filename of a template to use.
/reboot		Reboot the server after a template is applied.
/help|?		Show the help screen.

Here is an example that backs up the registry to a file named backup.reg, applies a custom template named MyServers.ictpl and reboots the server:

```
iiscryptocli /backup backup.reg /template "C:\temp\MyServers.ictpl" /reboot
```

Support

Please take a look at our FAQ. If you have any other questions, feel free to contact us.

Test Your Site

In order to test your site after you have applied your changes, click the Site Scanner but

Unieke FAQ ID: #1027
Auteur: diode
Laatst bijgewerkt:30-08-2023 11:19