TECH REVIEW

Secure Configuration for the Orion Platform

Version 2020.2.1

Last Updated: December 14, 2020

Table of Contents

Review Disclaimer

This review includes sections from the Administrator Guide. Please note:

- Page breaks are not final.
- Some links might not function because linked topics are not included in the sections being reviewed.
- Broken links, for example, URLs might be automatically generated by your PDF viewer (for example, in Adobe Acrobat, you might have the Create links from URLs item in General settings selected).

Best Practices for Your Orion Deployment

Recommendations

- Ensure you have installed the latest versions of the SolarWinds® Orion® Platform, including hotfixes and service releases.
- Maintain the latest host operating system, application, and network security updates.
- Be careful not to expose your Orion Platform website on the public internet.
- Disable unnecessary ports, protocols, and services on your host operating system and on applications, like SQL Server. See the Orion Port requirements guide for more information.
- Apply proper segmentation controls on the network where you have deployed the SolarWinds Orion Platform.
- Implement strict access control and auditing in your environment at operating system and network layers. Limit access to the Orion servers to only those authorized persons who require access as part of their duties.
- Apply layered network security controls, like leveraging application load balancers, setting appropriate firewall rules to limit who can access or send network traffic to your Orion Platform, and deploying security tools to provide additional monitoring across your Orion Platform environment.
- Purchase additional web servers for segregation and accessing the web console. Unlike your primary polling engine, these do not run many critical services. Once setup, you can disable IIS and web services on your primary polling engine and allow the rest of the services to function independently of IIS.
- If you deploy multiple Orion servers in your environment, dedicate these servers where possible and minimize the installation of any third-party software.
- Do not create local Orion-based accounts. We recommend at minimum utilizing Windows Authentication, or implementing a SAML v2 based solution, if you cannot integrate Windows or SAML-based authentication.
- Ensure you configure account settings and leverage both account and view limitations, along with module-specific roles only for the tasks they require in their role.

Secure Configuration for the Orion Platform

This document describes configuration options for securing your Orion Platform deployment.

Security option	Version	Default settings
HTTPS	2017.1 +	Enabled by default if a suitable certificate is found. » Show me how Recommendations: • 2,048 bits for RSA (~112-bit security) or 256+ bits for ECDSA (128-bit security). • Over 2,048 bits, use ECDSA. • Renew certificates regularly. • Sign certificates with SHA 256 or higher.
HSTS	2018.4 +	Disabled by default » Show me how to enable this
CSRF	2018.4 +	*_AntiXSRFToken* enabled by default *XSRF-TOKEN* disabled by default » Show me how to enable this
Secure Cookies	2018.4 +	Enabled by default » Show me how
Session Management	2020.2 +	Enabled by default » Show me how
TLS and Cipher Suites	2019.4 +	Settings required » Show me how
TLS Certificate Validation	2019.2 +	Disabled by default » Show me how to enable
SAML Signing	2018.4 +	Disabled by default » Show me how to enable this
Sensitive Exception Details	2019.2 +	Disabled by default » Show me how to disable this
Server Information Headers (Banner)	2020.2 +	» Show me how to set this
IIS Request Filtering	2020.2 +	See the KB IIS handler mapping.
Session Timeouts	All	» Show me how to set this

HTTPS

Supported by Orion Platform 2017.1 and later

HTTPS is configured on fresh installs only when a suitable certificate is found on the system. SolarWinds recommends you do not use a self-signed certificate.

Recommendations for certificates

- SolarWinds recommends using strong private keys: 2,048 bits for RSA (~112 bits of security) or 256+ bits for ECDSA (128 bits of security).
- RSA doesn't scale well above 2,048, so after that, ECDSA should be preferred.
- Renew certificates (including private keys) regularly, because revocation mechanisms are not reliable.
- Sign your certificates with SHA256 or higher.

How to enable

1. Run the Configuration wizard, click Next to use defaults until you reach the Website Settings step.
2. Select the Enable HTTPS option. See Configure the Orion Web Console to use HTTPS for details.

HSTS

Supported by Orion Platform 2018.4 and later

HTTPS Strict Transport Security (HSTS) protects your deployment against protocol downgrade attacks (MITM SSL strip). HSTS headers instruct a client's browser to communicate only on HTTPS for a specified period of time. Orion uses one (1) year as a default.

How to enable

1. In the Orion Web Console, click Settings > All Settings, and then click Web Console Settings in the Product Specific Settings (/Orion/Admin/Settings.aspx).
2. Select the STRICT TRANSPORT SECURITY (HSTS) option and submit your changes.

CSRF Protection

Supported by:

- Orion Platform 2018.4 -2019.4 (not by default)

- Orion Platform 2020.2 and later (supported by default)

Cross-Site Request Forgery (CSRF) is an attack where the user performs unwanted action while being authorized. Orion uses two separate CSRF tokens/cookies.

- __AntiXSRFToken - Used by ASP.NET for postback validation, validation enabled by default
- XSRF-TOKEN - Used by .asmx and WebAPI, validation disabled by default

How to enable

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx
2. Select the EnableXsrfProtection option and save your changes.

Secure Cookies

Supported by Orion Platform 2018.4 and later

Secure flag helps to protect cookies from MITM attacks. This is enabled by default.

How to enable

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx
2. Select the EnableCookieSecureFlag option and save your changes.

Session Management

Supported by Orion Platform 2020.2 and later (enabled by default)

To prevent session fixation attacks and provide persistent logout. Session management binds the session ID with its owner and validates it on each request. It manages the session lifecycle from login, logout, and expiration.

How to enable

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx
2. Select the EnableSessionCoupling option and save your changes.

TLS and Cipher Suites

Supported by Orion Platform 2019.4 and later

See TLS Compatibility with Orion Platform products for details.

How to enable

SolarWinds recommends that you enable TLS machine-wide. You can use IISCrypto or alter Windows registry keys on your own:

- IIS Crypto (© 2020 Nartac Software, obtained from https://www.nartac.com/Products/IISCrypto on October 1, 2020).
- Restrict the use of certain cryptographic algorithms and protocols in Schannel.dll (© 2020 Microsoft, obtained from https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc on October 1, 2020).

> It is also possible to configure protocols for Orion services only.

RabbitMQ

You can configure all cipher suites that RabbitMQ accepts (and which TLS version) in \ProgramData\SolarWinds\Orion\RabbitMQ\rabbitmq.config configuration file.

Go to the *ssl_options* section and find the following subsections:

- *_ciphers*: You can set cipher suites that RabbitMQ accepts, these should correspond with your system-wide settings (set by IIS Crypto).
- *_versions*: You can specify TLS versions here.

See TLS Support for details (© 2007-2020 VMware Inc. or its affiliates, obtained from https://www.rabbitmq.com/ssl.html#tls-versions on October 1, 2020).

> SolarWinds uses the classic config format of the config file (there is section on how the setting of cipher suites must look like).

Recommended Crypto setting

Global machine setting: NON DEFAULT

Server/Client Protocol: TLS 1.2

Ciphers: AES 128 / 128, AES 256/256

Hashes: SHA1, SHA256, SHA384, SHA512

Key exchanges: Diffie-Hellman, PKCS, ECDH (DHE Miminum key length 2048 bit)

RabbitMQ Config: DEFAULT

RabbitMQ config has two default cipher suites settings which are configured by FIPS Manager:

- **FIPS Mode On Ciphers**

  {dhe_rsa,aes_256_gcm,aead,sha384}

  {dhe_dss,aes_256_gcm,aead,sha384}

  {dhe_rsa,aes_256_cbc,sha256}

  {dhe_dss,aes_256_cbc,sha256}

  {dhe_rsa,aes_128_gcm,aead,sha256}

  {dhe_dss,aes_128_gcm,aead,sha256}

  {dhe_rsa,aes_128_cbc,sha256}

  {dhe_dss,aes_128_cbc,sha256}

- **FIPS Mode Off Ciphers**

  {ecdhe_rsa, aes_256_gcm, aead, sha384}

  {ecdhe_ecdsa, aes_256_gcm, aead, sha384}

  {ecdhe_rsa, aes_256_cbc, sha384, sha384}

  {ecdhe_ecdsa, aes_256_cbc, sha384, sha384}

  {ecdhe_rsa, aes_128_gcm, aead, sha256}

  {ecdhe_ecdsa, aes_128_gcm, aead, sha256}

  {ecdhe_rsa, aes_128_cbc, sha256, sha256}

  {ecdhe_ecdsa, aes_128_cbc, sha256, sha256}

  {ecdh_rsa, aes_256_gcm, aead, sha384}

  {ecdh_ecdsa, aes_256_gcm, aead, sha384}

  {ecdh_rsa, aes_256_cbc, sha384, sha384}

  {ecdh_ecdsa, aes_256_cbc, sha384, sha384}

  {ecdh_rsa, aes_128_gcm, aead, sha256}

  {ecdh_ecdsa, aes_128_gcm, aead, sha256}

  {ecdh_rsa, aes_128_cbc, sha256, sha256}

  {ecdh_ecdsa, aes_128_cbc, sha256, sha256}

{dhe_rsa, aes_256_gcm, aead, sha384}

{dhe_dss, aes_256_gcm, aead, sha384}

{dhe_rsa, aes_256_cbc, sha256}

{dhe_dss, aes_256_cbc, sha256}

{dhe_rsa, aes_128_gcm, aead, sha256}

{dhe_dss, aes_128_gcm, aead, sha256}

{dhe_rsa, aes_128_cbc, sha256}

{dhe_dss, aes_128_cbc, sha256}

TLS Certificate Validation

Supported by Orion Platform 2019.2 and later

As required by CC PP, TLS certificates should be fully validated.

How to enable

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx)
2. Select the following options and save your changes:

    - CheckOnCertificateChainErrors
    - CheckOnCertificateNameMismatch
    - CheckOnCertificateRevocation

SAML Signing

Supported by Orion Platform 2018.4 and later (not by default)

Applicable when single sign-on is used. By default, only one signature is required and validated (assertion or SAML response).

You can configure the Orion Platform to require a specific validation or both validations.

See Authenticate Orion Platform users with SAML v2 for configuration details.

How to enable

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx)
2. Select the following options and save your changes:
    - SamlAssertionSigningRequired
    - SamlResponseSigningRequired

Sensitive Exception Details

Supported by Orion Platform 2019.2 and later (not by default)

By default, only users with Administrator rights can see detailed exceptions. This setting protects you from disclosing sensitive information (variable names, SQL strings, system path information, and source/program code or call stacks) to Orion users.

How to disable

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx
2. Clear the IncludeErrorDetail option and save your changes.

Server Information Headers (Banner)

Supported by Orion Platform 2020.2 or later

Not to disclose server information in headers (Server - Specifies the webserver version. X-Powered-By - Indicates that the website is "powered by ASP.NET." X-AspNet-Version - Specifies the version of ASP.NET used), apply additional configuration on IIS.

How to configure

See Disable the IIS web banner and other IIS headers in the Orion Platform for details.

IIS Request Filtering

Supported by Orion Platform 2020.2.1 HF 2 or later

You can configure your IIS to allow only the required extensions for the application.

See https://support.solarwinds.com/SuccessCenter/s/article/IIS-handler-mapping-requirements?language=en_US for more details.

Session Timeouts

You can configure your Orion Platform sessions to time out after a shorter time than the default 25 minutes.

1. Log in to the Orion Web Console as an administrator and go to Advanced Configuration. Adjust the Orion Web Console URL as follows: [hostname]/Orion/Admin/advancedconfiguration/global.aspx
2. Change the SESSION TIMEOUT option and save your changes. The default is 25 minutes.

Secure external programs and script alerting actions

Supported by Orion Platform 2020.2.1 HF 2 or later

Starting with the Orion Platform 2020.2.1 Hotfix 2, You can now configure your Orion Platform alert actions to be run in the context of a limited user account.

See https://support.solarwinds.com/SuccessCenter/s/article/Secure-external-programs-and-script-alerting-actions?language=en_US for more details.

Secure SQL variables used in Orion Platform

Supported by Orion Platform 2020.2.1 HF 2 or later

Starting with the Orion Platform 2020.2.1 Hotfix 2, You can use the MacroParser-isSecuringSQLMacroEnabled setting to improve the overall security of your Orion Platform by restricting specific SQL macros.

See https://support.solarwinds.com/SuccessCenter/s/article/How-to-secure-SQL-variables-used-in-Orion-Platform for more details.