CUMULOCITY IoT

BY SOFTWARE AG

Security Hardening Guidelines

Release 10.13.0

Last updated: 04/14/2022

This content applies to Cumulocity IoT 10.13.0 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Table of Contents

1 Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Cumulocity IoT platform version up to 10.13.0. Ensure you are using the Security Hardening guide relevant to the version you use.

2 Intended audience

This document defines the security configuration guidelines from a tenant administration point of view and contains deployment security best practices.

The profile “Deployment Security” is intended for system administrators and the profile “Configuration Guidelines” are intended for Enterprise tenant administrators.

3 Profile definitions

The document contains two profiles: “Configuration Guidelines” and “Deployment Security”.

Configuration Guidelines: This profile is defined for Enterprise tenant administrators and ensures that the recommendations defined secure his tenant space and provide a safe browsing experience to its users.

Deployment Security: This profile is defined for system administrators who deploy the platform on their own infrastructure.

4 Recommendations

Deployment security best practices

Ensure that the operating system is hardened for security

Best practice ID:

C8Y_P_DS_BP_01

Description

System hardening, also called operating system hardening, is the process of securing a system by reducing its surface of vulnerability. It is done to minimize a computer operating system’s exposure to threats and to mitigate possible risks.

Audit

Verify if the OS security hardening script execution is enabled. By default, execution of the OS security hardening script is disabled.

```
"cumulocity-os-update" => {
  "os-hardening" => {
    "enabled" => false,
    "script-path" => "/tmp/sag-os-security-hardening-script.sh"
```

If the enabled option is found to be ‘false’ then it is a finding.

Remediation

Enable OS hardening script execution after OS patching. This can be done by configuring the OS-hardening option in Chef environment file as follows:

```
"cumulocity-os-update" => {
  "os-hardening" => {
    "enabled" => true,
    "script-path" => "/tmp/sag-os-security-hardening-script.sh"
```

The execution of the OS security hardening script requires at least one of three triggers used also for OS patching. For more details about enabling the OS hardening option and the triggers to be used, refer to the **Multi-node Installation guide**.

Ensure that the OS security patches are applied on a regular basis

Best practice ID:

C8Y_P_DS_BP_02

Description

It is a good practice to define a security patch management timeline and update OS components on a regular basis in order to apply the latest security patches.

Audit

Ensure your organization has a security patch management process in place. Verify that the following packages are excluded from upgrades as part of patch management.

> **Exclusion List:**
>
> “mongodb*”, “java*”", “systemd*”, “cumulocity-_”, “nginx”, “_-agent-server*”, “epel-release”, “python2-boto”, “nodejs*”,“openresty*”, “kube*”, “docker*”, “python34-pytoml”

If your organization has an automated patch management process and if the above-mentioned components are not excluded from upgrade, then it is a finding.

Remediation

Have a patch management process and ensure that the process excludes the components from upgrade as defined in _Upgrading the Cumuloctiy IoT platform > Apply OS Security patches_ in the Core Multi-node installation guide.

Ensure that the platform is up to date

Best practice ID:

C8Y_P_DS_BP_03

Description

The Cumulocity IoT platform is upgraded with the latest features and security improvements with every release. It is important that you keep your platform up to date and ensure that the version in use is secure and is in the list of supported versions by Cumulocity IoT. Details about the release types can be found here.

Audit

Verify that the version in use is supported by Cumulocity IoT. Product version availability can be found here. Verify that the version in use is the latest version.

If you are using an old and unsupported version, it is a finding.

Remediation

Ensure your organization has defined an upgrade procedure and it follows _Upgrading the Cumulocity IoT platform_ in the Core Multi-node installation guide.

Ensure only the required ports are exposed

Best practice ID:

C8Y_P_DS_BP_04

Description

While there are many internal components in the platform, not all of them need to be exposed. If you have the platform deployed behind an external firewall or load balancer, it is important to understand the list of ports that needs to be exposed to the external world. By default, the platform expects the following ports to be opened at the external firewall in order to accept traffic from users and devices on the internet.

```
Ports: 443(HTTPS), 1883(MQTT), 8883(MQTT/TLS)
```

It is important to understand that port 80 and port 1883 are unsecured ports and allow unencrypted traffic.

Audit

Verify the open ports on the external firewall. If any ports other than 443 and 8883 are accessible, then it is a finding.

Remediation

Ensure all the ports except 443 and 8883 are closed.

Exception:

- There is a possibility to open additional ports to handle the MQTT traffic without ip_hash. The load balancer will use the standard round-robin algorithm instead. These additional ports need to be enabled on the firewall as well.

TLS/SSL deployment best practices

SSL/TLS is a deceptively simple technology. The main problem is that encryption is not often easy to deploy correctly. To ensure that TLS provides the necessary security, system administrators and developers must ensure that the certificates are procured from the right source and the platform is configured properly.

Ensure all the default account passwords created are complex enough

Best practice ID:

C8Y_P_DS_BP_05

Description

Strong passwords are absolutely important. They prevent unauthorized access to your user accounts and devices. The more complex your password is, the more security it provides for your account. During installation, many components require admin password or default password changes. As an administrator, ensure that the password complexity meets the minimum complexity requirements:

- Include lowercase characters, such as “abcdef”
- Include uppercase characters, such as “ABCDEF”
- Include numbers, such as “123456”
- Include symbols, such as “!@#$%^”
- Must have at least 8 characters

Audit

1. Verify that the password for NEXUS repository is changed. Check if the default credentials (username: admin, password: admin123) is in use.
2. Verify the Chef admin user password.
3. Verify the mongodb.password and mongodb.initPassword values are set in Chef environment files on the Chef server.
4. Verify the following passwords in Chef environment files:
    - “management.admin.password”
    - “tenant.admin.password”
    - “admin.password”
    - “sysadmin.password”

If any of the above passwords don’t meet the password complexity requirements, then it is a finding.

Remediation

During the installation process, make sure the complex passwords are used. The configuration details are explained in the *Installation overview* in the Core Multi-node installation guide.

Ensure that you prevent the platform from creating sysadmin users for new tenants

Best practice ID:

C8Y_P_DS_BP_06

Description

The sysadmin user can become a potential backdoor for your tenant and it is recommended that while deploying the platform, you configure the platform to prevent creating sysadmin users for the new tenants.

Audit

Verify if the sysadmin.password param is set to EMPTY in the Chef environment file. If the value is set with a password, then it is a finding.

Remediation

Make sure that the sysadmin.password param is set to EMPTY in the environment file. Refer to *Backend installation > Example environment configuration* in the Core Multi-node installation guide.

Ensure that the deployed custom SSL certificates are secure and produced from a reliable CA

Best practice ID:

C8Y_P_DS_BP_07

Description

The Cumulocity IoT platform needs to be configured with digital certificates to support secure communication through TLS/SSL. This section details best practices regarding the creation of certificates and getting them signed from a Certifying Authority (CA).

Audit

Verify the following parameters while procuring the certificate for your organization:

- Verify the domain name. Ensure the common name is configured to suit all your sub-domains.
- Verify the private key length. It should be at least 2048 bit.
- Verify the Certificate Authority (CA) who signed your domain certificate is reliable.
- Verify that the certificate is signed using a strong signature algorithm.

Any deviation from the above can be considered a finding.

Remediation

Some of the best SSL Certificate Authorities you can procure certificates from include but aren’t limited to: *DigiCert SSL*, *Comodo SSL*, *RapidSSL*, *Thawte SSL*, *Sectigo SSL*, *GeoTrust SSL* and *Symantec SSL*.

Ensure that the Nginx server is configured to use secure TLS Protocols

Best practice ID:

C8Y_P_DS_BP_08

Description

To provide a high degree of privacy, SSL/TLS encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a mix of characters that is nearly impossible to decrypt. It is important to support strong TLS protocols on your webserver as there are many known attacks and exploits available for weaker protocols.

Audit

Verify the following section of the external-lb configurations in the Chef environment file:

```
"cumulocity-external-lb" => {
  "ssl_ciphers" => "HIGH !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4 !MD5"
  "ssl_protocols" => "TLSv1.2 TLSv1.3"
  (...)
}
```

If the “ssl_protocols” attribute contains any version other than TLSv1.2 or TLSv1.3, then it is a finding.

Remediation

Ensure only TLSv1.2 and TLSv1.3 is configured for “ssl_protocols” attribute in Chef environment file.

The configuration details are explained in *Load balancer configuration guidelines > HTTPS - Recommendations for TLS/SSL Protocol & Cipher Hardening* in the Core Operations guide.

> **Info:** Configuring Nginx to support only strong protocols and ciphers could cause connectivity issues to some legacy devices. Hence, configure the above properties based on the business needs.

Ensure that the Nginx server is configured to use secure cipher suites

Best practice ID:

C8Y_P_DS_BP_09

Description

To provide a high degree of privacy, SSL/TLS encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a mix of characters that is nearly impossible to decrypt. Together with strong TLS protocols, it is important that you configure your webserver to support only strong cipher suites.

Audit

Verify the following section of the external-lb configurations in the Chef environment file:

```
"cumulocity-external-lb" => {
  "ssl_ciphers" => "HIGH !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4 !MD5"
  "ssl_protocols" => "TLSv1.2 TLSv1"
  (...)
}
```

Alternatively, you can make use of tools like SSLyze https://github.com/nabla-c0d3/sslyze or TestSSLServer http://www.bolet.org/TestSSLServer/ to verify the list of weak ciphers supported by Nginx.

Remediation

Ensure only strong ciphers are configured for “ssl_ciphers” attribute in the Chef environment file. The configuration details are explained in *Load balancer configuration guidelines > HTTPS - Recommendations for TLS/SSL Protocol & Cipher Hardening* in the Core Operations guide.

> **Info:** Configuring Nginx to support only strong protocols and ciphers could cause connectivity issues to some legacy devices. Hence, configure the above properties based on the business needs.

Ensure the maximum number of failed user login requests is configured

Best practice ID:

C8Y_P_DS_BP_10

Description

Account lockout is a useful method for slowing down online password guessing attacks as well as to compensate for weak password policies. These three policies work together to limit the number of consecutive login attempts that fail due to a bad password within a period of time. While it is important to enforce password complexity on users, it is equally important to disable the user accounts that are identified to be under attack. The platform offers features to configure the maximum number of consecutive failed user login attempts after which the user will be disabled.

Audit

Ensure your organization policy has a defined account lockout policy for its users. Make sure that the badRequestCounter property set in cumulocity-core.properties file matches to the value defined by your organization. This value is defaulted to 100 per core. If there is a deviation observed in the value set to the defined value, then it is a finding.

Remediation

As the cumulocity-core.properties file is managed by Chef, you need to add the following entry to the Chef environment description. Adjust the value as required by your business needs.

```
...
"cumulocity-core" => {
  "properties" => {
  ...
  "system.authentication.badRequestCounter" => "70",
  ...
  }
}
...
```

More details about this configuration can be found in *Operational procedures > Configure maximum number of failed user login requests* in the Core Operations guide.

Ensure TFA is enforced globally for ‘admin’ groups

Best practice ID:

C8Y_P_DS_BP_11

Description

The two-factor authentication can be enforced on all the tenant users at a global level. This global two-factor authentication is to be configured through Chef server configuration. It is a good practice that you enable the TFA for all the users with privileged roles. By default, this configuration is disabled, and it is recommended that the platform administrators enable two-factor authentication for all the admin users.

Audit

Review the Chef environment file. Verify the value set for the property “system.two-factor-authentication.enabled”. If it is set to false, then it is a finding.

Remediation

Add the following entries to the Chef environment file for the system and import it into the Chef server:

```
...
"cumulocity-core" => {
  "properties" => {
  ...
  "system.two-factor-authentication.enabled" => false,
  "system.two-factor-authentication.enforced.group" => "admins",
  ...
  }
}
```

The entry “system.two-factor-authentication.enforced.group” lists the groups for which the two-factor authentication is enforced.

Ensure that an endpoint protection solution is deployed

Best practice ID:

C8Y_P_DS_BP_12

Description

The need for effective endpoint security measures has increased substantially, particularly in light of a digital platform offering connectivity to a multitude of devices where there are chances for threat intrusion. Hence it is important that one considers the deployment of endpoint security protection on all platform nodes.

Audit

Verify if your deployment is configured with any endpoint protection solution that offers protection such as intrusion prevention, malware analysis, integrity monitoring and application control. If there is no endpoint protection solution deployed, then it is a finding.

Remediation

Consider deploying endpoint protection solutions such as Trendmicro or Crowdstrike or similar, that offers security capabilities such as intrusion prevention, anti-malware, integrity monitoring, log inspection, or application control.

> **Info:** The endpoint protection agents tend to utilize a lot of resources which might cause a performance drop. Select the endpoint protection solution that works best for your organization.

Ensure that a centralized audit logging system and SIEM is integrated to the platform

Best practice ID:

C8Y_P_DS_BP_13

Description

Centralized logging provides two important benefits. First, it places all the log records in a single location, greatly simplifying log analysis and correlation tasks. Second, it provides you with a secure storage area for your log data. In case that a machine on your network becomes compromised, the intruder will not be able to tamper with the logs stored in the central log repository. SIEM is important because it makes it easier for enterprises to manage security by filtering massive amounts of security data and prioritizing the security alerts the software generates. SIEM software enables organizations to detect incidents that may otherwise go undetected.

Audit

Verify if the deployment architecture includes a central logging system and SIEM capabilities.

Remediation

Ensure the deployment includes a central logging system with SIEM capabilities like Graylag or Splunk or similar.

Ensure that you are subscribed for security alerts and advisories in Empower

Best practice ID:

C8Y_P_DS_BP_14

Description

Software AG publishes early warnings and critical alerts in its customer portal called “Empower”. This includes information regarding security advisories, the critical fixes that are released and the latest security patches. You will get the notifications only if you have subscribed for alerts. Hence it is important that the system administrators and operation administrators subscribe to the early warnings published to take the necessary action on their environments.

Audit

Verify if the administrator has subscribed for early warnings in Empower. If not ensure you have subscribed for it in Empower.

Remediation

Subscribe to Cumulocity IoT alerts in Empower.

Tenant administration - Security configuration guidelines

Ensure the authentication mode is set to OAI-Secure

Best practice ID:

C8Y_P_TM_CG_01

Description

While the default authentication is set to basic authentication, OAI-Secure authentication offers more security control like session management, two-factor authentication, and audit controls.

Audit

Login as tenant administrator and navigate to **Administration** > **Settings** > **Authentication**. Verify if the preferred login mode is set to OAI-Secure. If OAI-Secure is not set as login mode, then it is a finding.

Remediation

Login as tenant administrator and change the login mode to OAI-Secure.

Ensure the password validity limit is configured

Best practice ID:

C8Y_P_TM_CG_02

Description

By default, the tenant user passwords are configured not to expire. With growing computational power, it becomes easier to crack the passwords if they are not frequently changed. The platform offers a feature to configure the password expiry interval as required by business.

Audit

Verify if you have an organization policy defined for configuring the password validity. Login as tenant administrator and navigate to **Administration** > **Settings** > **Authentication**. Verify the value configured for “Limit password validity for” field. If there is a deviation to the value defined by your organization, then it is a finding.

Remediation

The recent security research recommends not to configure any password expiry because of its debatable benefit. Ensure you pay due diligence while configuring and match your business requirements.

Ensure that strong passwords are enforced for all the users in the platform

Best practice ID:

C8Y_P_TM_CG_03

Description

The password complexity can be defined and enforced by the management tenant admin. If for some reason the tenant admin decides not to enforce password complexity on all the tenants, then it becomes the tenant admin’s responsibility to enforce strong passwords for all its users. The password complexity in the platform is defined to include the following:

- Include lowercase characters, such as “abcdef”
- Include uppercase characters, such as “ABCDEF”
- Include numbers, such as “123456”
- Include symbols, such as “!@#$%^”
- Must have at least 8 characters

Audit

Login as tenant administrator and navigate to **Administration** > **Settings** > **Authentication**. Verify if the option “Enforce that all the passwords are strong (green)” is checked. If the option is not checked, then it is a finding.

Remediation

As a best practice, it is recommended to enforce strong passwords. Check the option “Enforce that all the passwords are strong (green)”.

Ensure that two-factor authentication is enforced for all users

Best practice ID:

C8Y_P_TM_CG_04

Description

The two-factor authentication (TFA) can be defined and enforced by the management tenant admin. If for some reason, the tenant admin decides not to enforce TFA, it becomes the responsibility of the Enterprise Tenant admin to enforce TFA.

For users managed by tenant admins the platform offers an option to configure TOTP based TFA.

When TFA is disabled on system level you can still activate it on tenant level using the UI.

Audit

Login as tenant administrator and navigate to **Administration** > **Settings** > **Authentication**. Verify if the option “Allow two-factor authentication” is checked. Verify if the “Google Authenticator (TOTP)” option is checked. Verify if the option “Enforce two-factor authentication” is checked.

If any of the values is not checked, then it is a finding.

Remediation

Login as tenant administrator and check the option “Enforce two-factor authentication for all users”.

Ensure that two-factor authentication is enforced for users with privileged roles

Best practice ID:

C8Y_P_TM_CG_05

Description

TFA can be enabled for all the users in the tenant space. But it may not be relevant in all cases to enforce TFA for all users but to enforce it only on users with privileged roles. The platform offers tenant admins a feature to enforce TFA for specific users.

Audit

Login as tenant administrator and navigate to **Administration** > **Accounts** > **Users**. Mark all the users assigned with privileged roles. Navigate to every user and verify if the option “Enforce TOTP setup for the user” is checked.

If the “Enforce TOTP setup for the user” is not checked, then it is a finding.

Remediation

Login as tenant administrator and check the option “Enforce TOTP setup for the user” for all users with privileged roles.

Ensure that JWT session token validity time is configured properly

Best practice ID:

C8Y_P_TM_CG_06

Description

Cumulocity IoT OAI-Secure is based on a JWT stored in a browser cookie. However, it doesn’t support refresh and after the token validity time has ended, the user will have to log in again. The default token validity time is two weeks but is configurable. The minimum allowed value is 5 minutes.

Audit

Verify if your organization has a defined a policy for session timeout. Login as tenant administrator. Verify the cookie attribute “authorization”. This is a JWT token. Decode this token using any online tool, for example, https://jwt.io). Verify the “exp” value in the payload. Verify the cookie expiration value.

If the value configured deviates from the one that is defined in your organization policy, then it is a finding.

Remediation

Login as tenant administrator and configure the following tenant options as defined in your organization policy:

- token-lifespan
- cookie-lifespan

For example, if you want to set these values to 10 minutes, configure the above options to 600 seconds. To configure the tenant options, call the following POST request using tenant admin credentials:

```
URL: {{url}}/tenant/options
Body :
{
  "category": "oauth.internal",
  "key": "basic-token.lifespan.seconds", //or “basic-user.cookie.lifespan.seconds”
  "value": "600"
}
```

Ensure that the roles with appropriate permissions are created

Best practice ID:

C8Y_P_TM_CG_07

Description

Permissions define what a user is allowed to do in Cumulocity IoT applications. To manage permissions more easily, they are grouped into roles. There are pre-defined global roles that are not fully configured. These global roles can only be considered samples which are pre-configured for a particular purpose. You may use them as a starting point and further adapt them to your individual needs.

Audit

Ensure your organization has a set of roles defined with appropriate permissions. Login as tenant administrator and navigate to **Administration** > **Accounts** > **Roles**. Verify if the roles are created as defined. Navigate to every role and verify if the permissions are assigned as defined.

If there are deviations observed from what is defined and what is configured, then it is a finding.

Remediation

The platform offers features to create custom roles and customize the permissions. Ensure your organization has defined ACLs as required for business and the same is reflected in the configurations.

Ensure CORS is configured appropriately

Best practice ID:

C8Y_P_TM_CG_08

Definition

Tenant administrators can enable cross-origin resource sharing (CORS) for the Cumulocity IoT API. This configuration enables the JavaScript web applications to directly communicate with REST APIs deployed on the platform.

Options available:

- Enter “*” to allow communication from any host.
- Enter “http://my.host.com”, “http://myother.host.com” to allow applications from “http://my.host.com” and from “http://myother.host.com” to communicate with the platform.
- Leave the field blank to allow access only from your tenant’s domain.

Audit

Login as tenant administrator and navigate to **Administration** > **Settings** > **Application**. In the access control section, verify the value configured for “Allowed Domain”. If the value is set to “*”, then it is a finding.

Remediation

Configure the “Allowed Domain” field only with the trusted domains, from where you want to access the REST APIs hosted on platform.

Ensure the subtenant requests rate limits are configured

Best practice ID:

C8Y_P_TM_CG_09

Description

Rate limiting is an important feature to ensure that the tenants are accessing the resources in the agreed limits. These limits prevent users and devices from creating a flood of requests intentionally or unintentionally. This prevents attacks like denial of service (DoS) or request flooding. Tenant administrators can limit the request rate of each subtenant via the following custom properties:

- Limit HTTP queue - Limit of HTTP request queue for tenant
- Limit HTTP requests - Limit of HTTP requests for tenant per second
- Limit stream queue - Limit of MQTT request queue for tenant
- Limit stream requests - Limit of MQTT requests for tenant per second

Audit

Ensure your organization has defined the rate limits for all its subtenants. Login as tenant administrator and navigate to **Administration** > **Tenants** > **Subtenants**. For every subtenant go to **Custom properties** tab. Verify the values set for the following fields:

- Limit HTTP requests
- Limit HTTP queue
- Limit stream requests
- Limit stream queue

When there is no limit set or it is set to “-1”, the limit feature is considered disabled and the tenant gains unlimited access. This is a finding.

Remediation

Configure the above-mentioned fields with a non-negative integer to ensure the rate limiting is configured and doesn’t expose the platform to attacks like request flooding or denial of service.

Ensure a limit is configured for subtenant device numbers

Best practice ID:

C8Y_P_TM_CG_10

Description

Tenant administrators can limit the count of concurrently registered root devices or simply all devices (including child devices) via the custom property “Limit number of devices”. This helps in controlling the device count of subtenants and allows better governance.

Audit

Ensure your organization has defined the rate limits for all its subtenants. Login as tenant administrator and navigate to **Administration** > **Tenants** > **Subtenants**. For every subtenant, go to **Custom properties** tab. Verify the values set for “Limit number of devices”.

If the value is not set or it is set to “-1”, then it is a finding.

Remediation

Configure the field “Limit number of devices” with a non-negative integer to ensure better governance on the number of devices connected to the platform at subtenant level.

Ensure a periodic review of subtenants and applications subscribed by subtenants

Best practice ID:

C8Y_P_TM_CG_11

Definition

As tenant administrator you will need to govern the set of subtenants under you tenant space and the applications they are subscribed to. This governance is important because you do not want to have extra subtenants in your space and want to ensure that they are subscribed only to the applications they are supposed to have access to.

Audit

Ensure your organization maintains a list of subtenants and their application subscriptions. A periodic review should be done on the tenant space to ensure there are no rogue tenants and the application subscriptions are appropriate.

Login as tenant administrator and navigate to **Administration** > **Tenants** > **Subtenants**. For ever subtenant, go to the **Applications** tab. Verify if they are subscribed only to applications they are entitled to.

If there are deviations observed from what is defined and what is configured, then it is a finding.

Remediation

NA

Ensure custom SSL certificates deployed are secure and procured from reliable CA while re-branding

Best practice ID:

C8Y_P_TM_CG_12

Description

The Cumulocity IoT platform offers features to customize the UI, domain names and the domain certificates. You can configure the SSL certificates for your custom domain thus enabling a completely customized user experience. As a tenant administrator it is your responsibility to configure secure SSL certificates for your customized domain.

Audit

Verify the following parameters in the certificate procured by your organization from the CA:

- The domain name. Ensure the common name is configured to suit all your sub-domains.
- The private key length. It should be at least 2048 bit.
- The Certificate Authority (CA) who signed your domain certificate and should be reliable.
- The certificate. It should be signed using a strong signature algorithm.

Any deviation observed from the above can be considered as a finding.

Remediation

Some of the best SSL Certificate Authorities you can procure certificates from include but aren’t limited to: *DigiCert SSL*, *Comodo SSL*, *RapidSSL*, *Thawte SSL*, *Sectigo SSL*, *GeoTrust SSL* and *Symantec SSL*.

5 Appendix

Summary table

Recommendation ID	Summary	Compliant (Yes/No/NA)
Deployment security best practices		
C8Y_P_DS_BP_01	Ensure that the Operating System is hardened for Security	
C8Y_P_DS_BP_02	Ensure that the OS security patches are applied on a regular basis	
C8Y_P_DS_BP_03	Ensure that the platform is up to date	
C8Y_P_DS_BP_04	Ensure only the required ports are exposed	
C8Y_P_DS_BP_05	Ensure all the default account passwords created are complex enough	
C8Y_P_DS_BP_06	Ensure the platform SSL certificates deployed are secure and procured from a reliable CA	
C8Y_P_DS_BP_07	Ensure the platform SSL certificates deployed are secure and procured from a reliable CA	
C8Y_P_DS_BP_08	Ensure that the Nginx server is configured to use secure TLS protocols	
C8Y_P_DS_BP_09	Ensure that the Nginx server is configured to use secure cipher suites	
C8Y_P_DS_BP_10	Ensure the maximum number of failed user login requests is configured	
C8Y_P_DS_BP_11	Ensure TFA is enforced globally for admin groups	
C8Y_P_DS_BP_12	Ensure that an endpoint protection solution is deployed	
C8Y_P_DS_BP_13	Ensure that a centralized audit logging system and SIEM is integrated to the platform	
C8Y_P_DS_BP_14	Ensure that you are subscribed for security alerts and advisories in Empower	
Tenant management configuration guidelines		

Recommendation ID	Summary	Compliant (Yes/No/NA)
C8Y_P_TM_CG_01	Ensure the authentication mode is set to OAI-Secure	
C8Y_P_TM_CG_02	Ensure the password validity limit is configured	
C8Y_P_TM_CG_03	Ensure that strong passwords are enforced for all users in the platform	
C8Y_P_TM_CG_04	Ensure that two-factor authentication is enforced for all users	
C8Y_P_TM_CG_05	Ensure that two-factor authentication is enforced for users with privileged roles	
C8Y_P_TM_CG_06	Ensure that JWT session token validity time is configured properly	
C8Y_P_TM_CG_07	Ensure that the roles with appropriate permissions are created	
C8Y_P_TM_CG_08	Ensure CORS is configured appropriately	
C8Y_P_TM_CG_09	Ensure the subtenant request rate limits are configured	
C8Y_P_TM_CG_10	Ensure a limit is configured on the number of subtenant devices	
C8Y_P_TM_CG_11	Ensure a periodic review of subtenants and applications subscribed by subtenants	
C8Y_P_TM_CG_12	Ensure custom SSL certificates deployed are secure and procured from a reliable CA while re-branding	

References

1. Center for Information Security (CIS) Benchmarks
2. Cumulocity documentation
3. Cumulocity IoT Core - Multi-node Installation guid
4. Cumulocity IoT Core – Operations guide

6 Contacting product support

Product support for Cumulocity IoT is provided to licensed customers by the Software AG Global support team, who you can access on the Software AG Empower web site at https://empower.softwareag.com/. There you will find information about how to contact us via email or phone. Some services on this site may require your Empower login ID and password.

If you are using Cumulocity IoT on a trial basis, you can refer to our free Tech Community pages at http://techcommunity.softwareag.com/ for information sources such as user forums and FAQs.