ABB CYLON® TECHNICAL BULLETIN NO. 548
Issue Date: 14 May 2025

ASPECT® v3.08.04

Summary

The ASPECT v3.08.04 release includes a wide range of security and general usability improvements. These improvements result from rigorous security assessments and significantly strengthen ASPECT against potential threats.

Detail

DON'T EXPOSE YOUR DEVICES ON THE INTERNET

Although a comprehensive discussion of network security is far beyond the scope of this document, the following items provide a starting point for creating a secure equipment installation. Where available, users should always defer to the security policies of the hosting network organization.

1. Always ensure that the ABB Cylon® Building Energy Management System (BEMS) solution is deployed on an isolated network specifically designated for BEMS controls only, with no connections to external networks.
2. Strictly prohibit the connection of ABB Cylon® BEMS devices to networks that include security-critical IP devices, such as CCTV systems, any data-sensitive infrastructure or credit card terminals.
3. ABB Cylon® BEMS solutions should never be exposed to the Internet. Exposure turns your system into a potential target accessible by every individual and machine globally.
4. Adopt a zero-exposure policy for ABB Cylon® devices on the internet. Always prioritize security by limiting information exposure to the minimum necessary for operational functionality.
5. Mandate the use of Secure Virtual Private Networks (VPNs) for all remote access requirements and always employ a Firewall for services requiring internet connectivity. VPNs ensure that devices remain off the public internet while providing a secure and encrypted path for authorized users to access system functions.

For more details see HT0038 ASPECT, FBXi and CBXi System Network Security Best Practice

INSTALLATION

Note: ASPECT v3.08.04 is an irrevocable upgrade meaning if an ASPECT target has been upgraded to v3.08.04 it cannot be backed down to any pre-v3.08.04 release

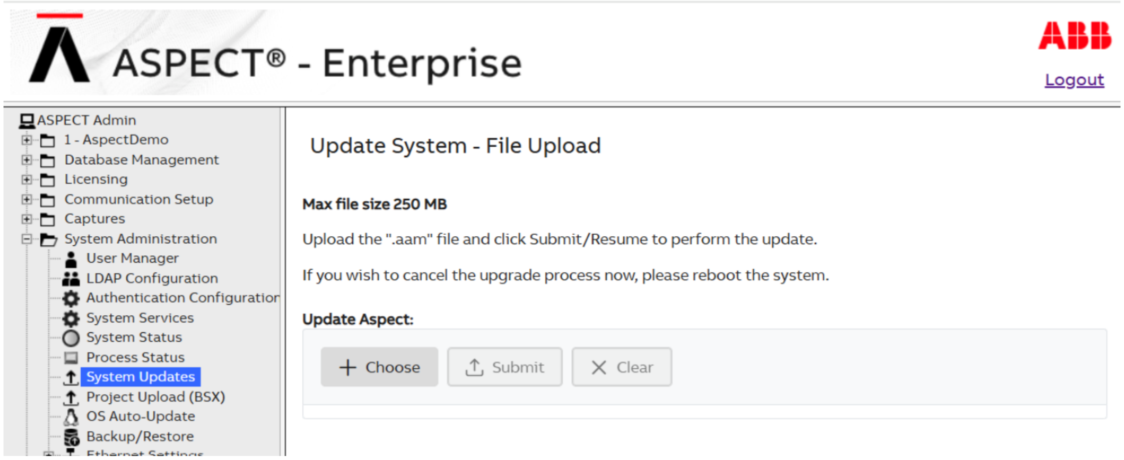
Note: ABB recommends closing all unnecessary ports on an ASPECT device.
After upgrading, always review port configuration for any unnecessarily open ports and close them accordingly.

FIRMWARE SECURITY UPGRADE

This release of ASPECT v3.08.04, requires a Security Patch to be installed prior to upgrading the firmware on an ASPECT target (MATRIX Series, NEXUS Series, ASPECT-Enterprise). The following patch will be included in the distribution bundle and must be installed before running the standard firmware upgrade on an ASPECT target:

- aspect-security-update_03.08.04.aam
- aspect-security-update_03.08.04.aam.sha256

Please install this bundle from the same upgrade menu option on the WebUI used to install the v`3.08.x` ASPECT bundles.



Update System - File Upload

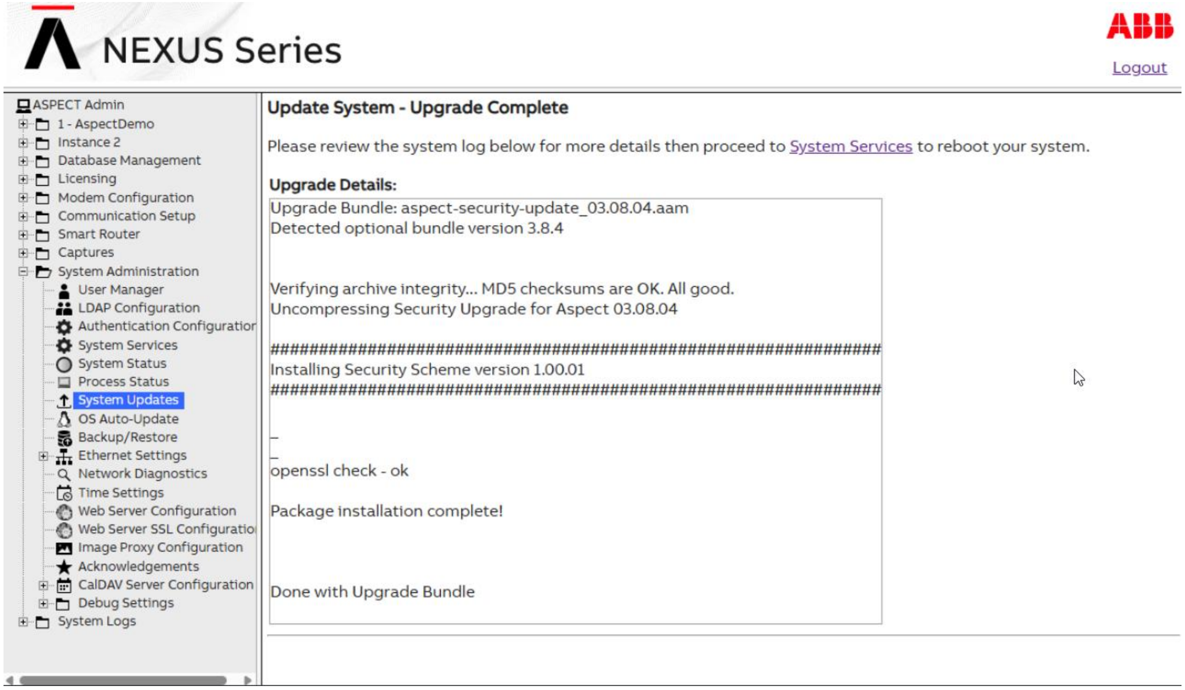
Max file size 250 MB

Upload the ".aam" file and click Submit/Resume to perform the update.

If you wish to cancel the upgrade process now, please reboot the system.

Update Aspect:

Look for the "Package installation complete!" message in the log window.



Update System - Upgrade Complete

Please review the system log below for more details then proceed to System Services to reboot your system.

Upgrade Details:

```
Upgrade Bundle: aspect-security-update_03.08.04.aam
Detected optional bundle version 3.8.4


Verifying archive integrity... MD5 checksums are OK. All good.
Uncompressing Security Upgrade for Aspect 03.08.04

########################################################################
Installing Security Scheme version 1.00.01
########################################################################


_
_
openssl check - ok

Package installation complete!



Done with Upgrade Bundle
```

Reboot the System

Finally restart/reboot the System from the System Services page.

Note: This security bundle is only required to be installed one time to support installation of secure firmware bundles for future releases of ASPECT.

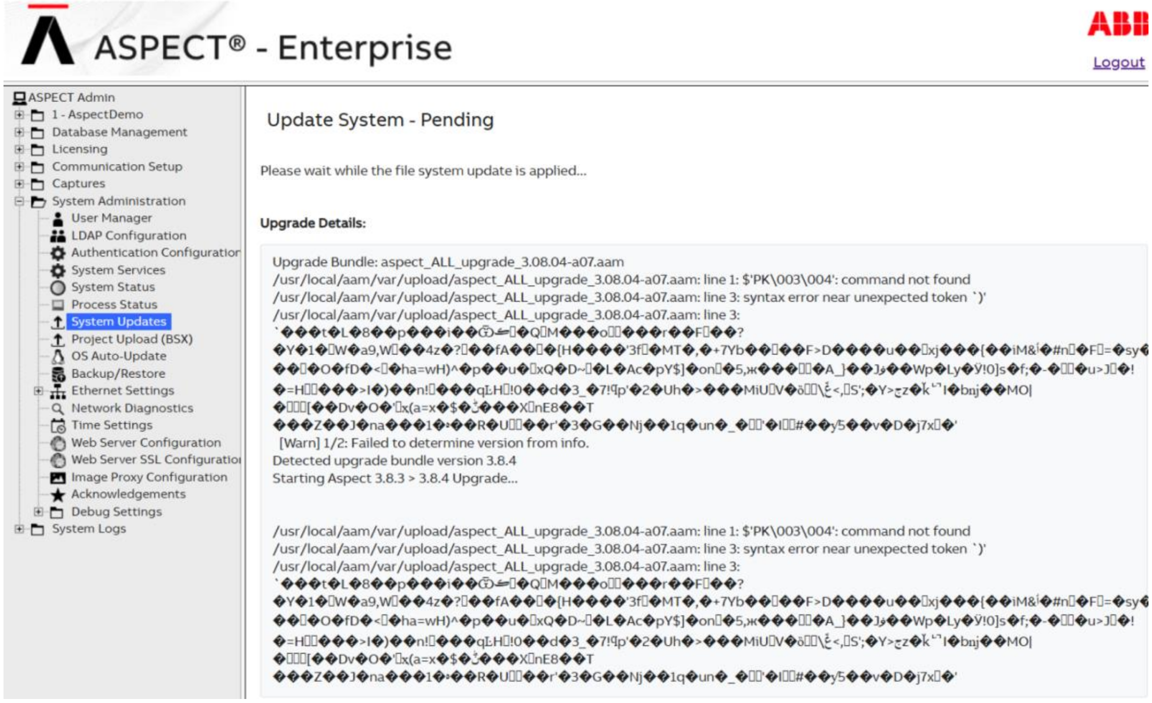
FIRMWARE UPGRADE

In order to take advantage of product enhancements and resolutions in **ASPECT** v`3.08.04`, you must upgrade the firmware of your existing **ASPECT** target (**MATRIX Series**, **NEXUS Series**, **ASPECT-Enterprise**) using the System Update feature within the `WebUI` of the target.

Instructions on this process can be found in the **ASPECT-Studio** Online Help at any time. Once your target's firmware has been updated, ***you must then open your existing project using*** **ASPECT-Studio** ***v***`3.08.04` ***and perform a Clean and then Deploy your project to the target being upgraded.*** This process <u>must</u> be done to ensure your project files receive all enhancements and updated drivers included as part of this maintenance release.

Install Notes:

The first time **ASPECT** firmware bundle v`3.08.04` is installed you must install the security bundle mentioned above ***first***. Failure to do this will result in the following update log message.



Update System - Pending

Please wait while the file system update is applied...

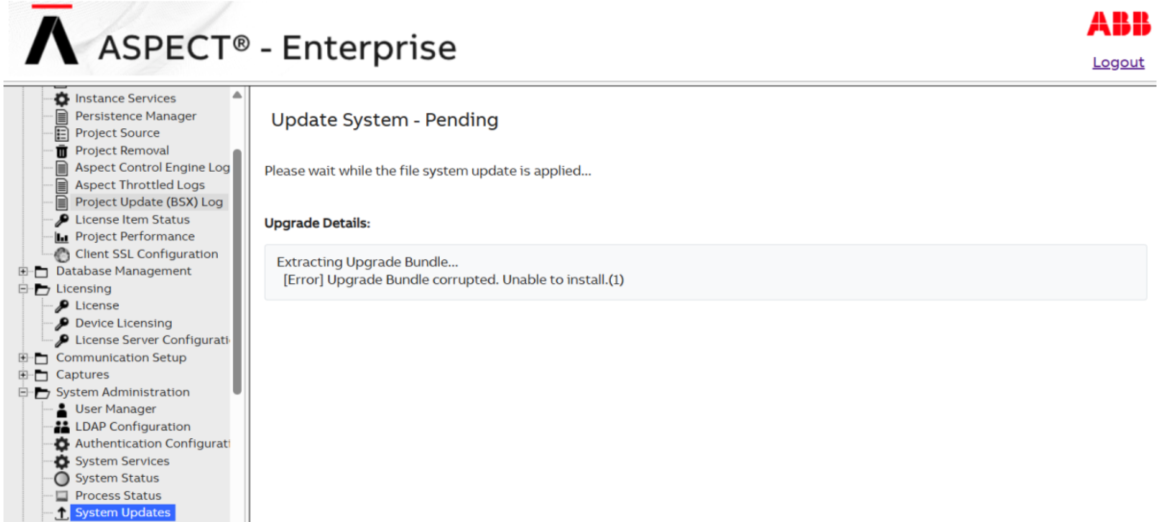
Upgrade Details:

```
Upgrade Bundle: aspect_ALL_upgrade_3.08.04-a07.aam
/usr/local/aam/var/upload/aspect_ALL_upgrade_3.08.04-a07.aam: line 1: $'PK\003\004': command not found
/usr/local/aam/var/upload/aspect_ALL_upgrade_3.08.04-a07.aam: line 3: syntax error near unexpected token `)'
/usr/local/aam/var/upload/aspect_ALL_upgrade_3.08.04-a07.aam: line 3:
`���t�L�8��p���i��ᏳD⥦▯�Q▯M���o▯▯���r��F▯��?
�Y�1�▯W�a9,W▯��4z�?▯��fA��▯�{H����'3f▯�MT�,�+7Yb��▯��F>D����u��▯xj���{��iM&ˡ�#n▯�F▯=�sy�
��▯�O�fD�<▯�ha=wH)^�p��u�▯xQ�D~▯�L�Ac�pY$]�on▯�5,ж���▯▯�A_}��Jؤ��Wp�Ly�Ÿ!0]s�f;�-�▯▯�u>J▯�!
�=H▯▯���>I�)��n!▯���qĿH▯!0��d�3_�7!¶p'�2�Uh�>���MiU▯V�ö▯▯\ڠ<,▯S';�Y>ݓz�ǩ˥˥I�bŋj��MO|
�▯▯▯[��Dv�O�'▯x(a=x�$�ڙ���X▯nE8��T
���Z��J�na���1�ּ��R�U▯▯��r'�3�G��Nj��1q�un�_�▯▯'�I▯▯#��y5��v�D�j7x▯�'
 [Warn] 1/2: Failed to determine version from info.
Detected upgrade bundle version 3.8.4
Starting Aspect 3.8.3 > 3.8.4 Upgrade...


/usr/local/aam/var/upload/aspect_ALL_upgrade_3.08.04-a07.aam: line 1: $'PK\003\004': command not found
/usr/local/aam/var/upload/aspect_ALL_upgrade_3.08.04-a07.aam: line 3: syntax error near unexpected token `)'
/usr/local/aam/var/upload/aspect_ALL_upgrade_3.08.04-a07.aam: line 3:
`���t�L�8��p���i��ᏳD⥦▯�Q▯M���o▯▯���r��F▯��?
�Y�1�▯W�a9,W▯��4z�?▯��fA��▯�{H����'3f▯�MT�,�+7Yb��▯��F>D����u��▯xj���{��iM&ˡ�#n▯�F▯=�sy�
��▯�O�fD�<▯�ha=wH)^�p��u�▯xQ�D~▯�L�Ac�pY$]�on▯�5,ж���▯▯�A_}��Jؤ��Wp�Ly�Ÿ!0]s�f;�-�▯▯�u>J▯�!
�=H▯▯���>I�)��n!▯���qĿH▯!0��d�3_�7!¶p'�2�Uh�>���MiU▯V�ö▯▯\ڠ<,▯S';�Y>ݓz�ǩ˥˥I�bŋj��MO|
�▯▯▯[��Dv�O�'▯x(a=x�$�ڙ���X▯nE8��T
���Z��J�na���1�ּ��R�U▯▯��r'�3�G��Nj��1q�un�_�▯▯'�I▯▯#��y5��v�D�j7x▯�'
```

Failed Aspect v3.08.04 Upgrade without Security Patch Applied

ASPECT v`3.08.04` is an **irrevocable upgrade** meaning if an Aspect target has been upgraded to v`3.08.04` it cannot be backed down to any pre-v`3.08.04` release. For example, if you want to back down to v`3.08.03` from v`3.08.04` the downgrade will fail as follows:



Update System - Pending

Please wait while the file system update is applied...

Upgrade Details:

```
Extracting Upgrade Bundle...
 [Error] Upgrade Bundle corrupted. Unable to install.(1)
```

Aspect v3.08.04 is a non-reversible upgrade

B0383 rev 7

Operating System Security Improvements

ASPECT v`3.08.04` has several security updates as well as an option to upload operating system patches to ASPECT devices running Linux CentOS 7.

ABB has partnered with a third party resource to provide core OS patches for CentOS 7 since it has entered End Of Life status. Patches on important core OS packages that rank a CVSS score of 7 or greater will be provided to customers on a quarterly basis from the security patch provider and will be downloadable from the ABB Toolbox.

IMPORTANT: Backup Your Project, Server Configuration and Database Prior to OS Upgrade

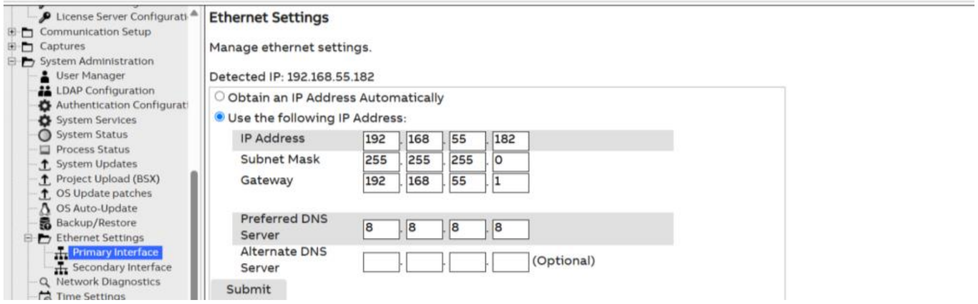
It is always good practice to make proper backups of the Project, Configuration and Database of an ASPECT target prior to doing any upgrade if they are not already available. Fresh backups can be made from the following pages on the ASPECT Web User Interface:

- **Project:** Project Instance → Project Source
- **Configuration:** System Administration → Backup / Restore
- **Database:** Database Management → MySQL Administration OR SQLite Maintenance

On-Line CentOS 7 End Of Life (EOL) Upgrade

In order to prepare an ASPECT CentOS 7 target to receive OS security patches, it must first be updated with all security patches provided by the CentOS Project up until it was declared End Of Life on June 30th 2024. These patches can be installed from the CentOS Vault repositories provided the following conditions are met:

- The ASPECT CentOS 7 Target Device or Enterprise VM has **"outgoing only"** access to the internet to access the CentOS Project vault repositories. Please work with your IT team to configure firewalls appropriately to allow outgoing access only.
- The ASPECT CentOS 7 target is configured with access to a DNS Server so that the yum upgrade package manager can locate the CentOS Project vault repositories.



Ethernet Settings

Manage ethernet settings.

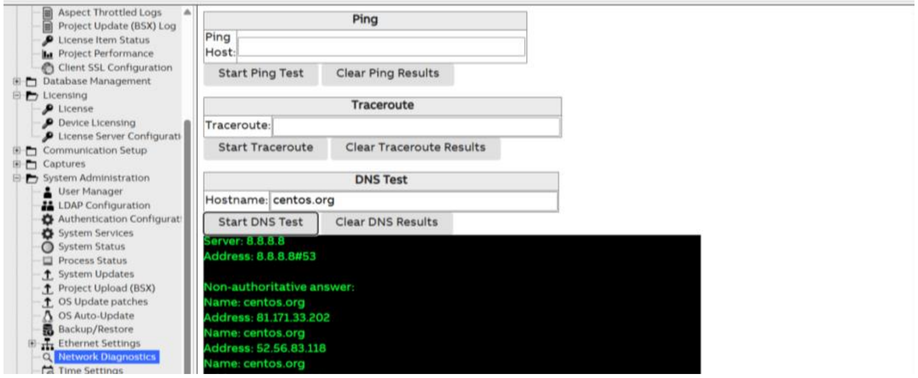
Detected IP: 192.168.55.182

○ Obtain an IP Address Automatically
● Use the following IP Address:

IP Address	192	168	55	182
Subnet Mask	255	255	255	0
Gateway	192	168	55	1
Preferred DNS Server	8	8	8	8
Alternate DNS Server				(Optional)

Configure Preferred DNS with a valid DNS Server

- Verify that the DNS Server can resolve Domain Names correctly



Ping Host:

Traceroute:

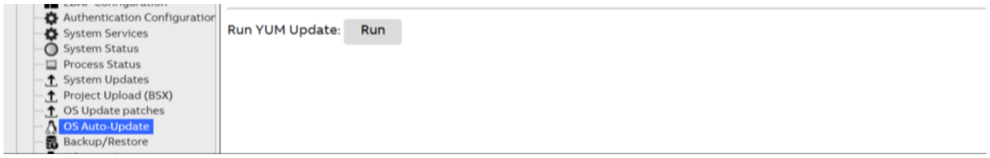
Hostname: centos.org

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: centos.org
Address: 81.171.33.202
Name: centos.org
Address: 52.56.83.118
Name: centos.org
```

Domain name centos.org resolved

- Once DNS Server has been confirmed to be accessible, manually run the YUM update by clicking on the "Run" button from the OS Auto Update page in the WebUI:



Run YUM Update: Run

Off-Line CentOS 7 End Of Life (EOL) Upgrade

If your device is in a siloed environment where the target has no access to the internet for End Of Life (EOL) upgrades, an off-line upgrade bundle is available from the ABB Community Toolbox.

Download Bundle:

- aspect_centos7_EOL_upgrade_v3.08.04.bundle.zip

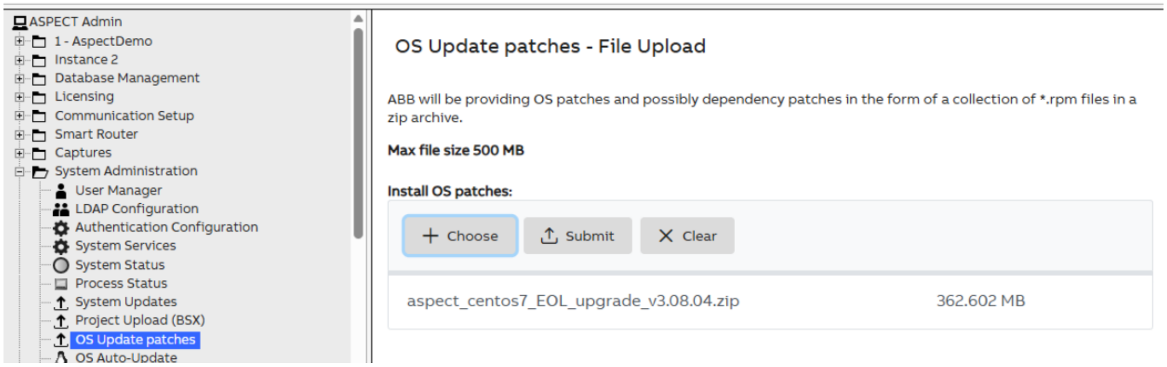
Unzip the upgrade bundle to extract the following files

- aspect_centos7_EOL_upgrade_v3.08.04.zip
- aspect_centos7_EOL_upgrade_v3.08.04.zip.sha256

Verify the integrity of the upgrade bundle by comparing the sha256 hash with the value in the *.sha256 file.

Finally, upload and run the upgrade bundle from the OS Update patches menu option in the ASPECT WebUI.

Note: Be careful to make sure not to upload the full bundled zip file (aspect_centos7_EOL_upgrade_v3.08.04.bundle.zip) file directly to the target device as this will result in an error.



OS Update patches - File Upload

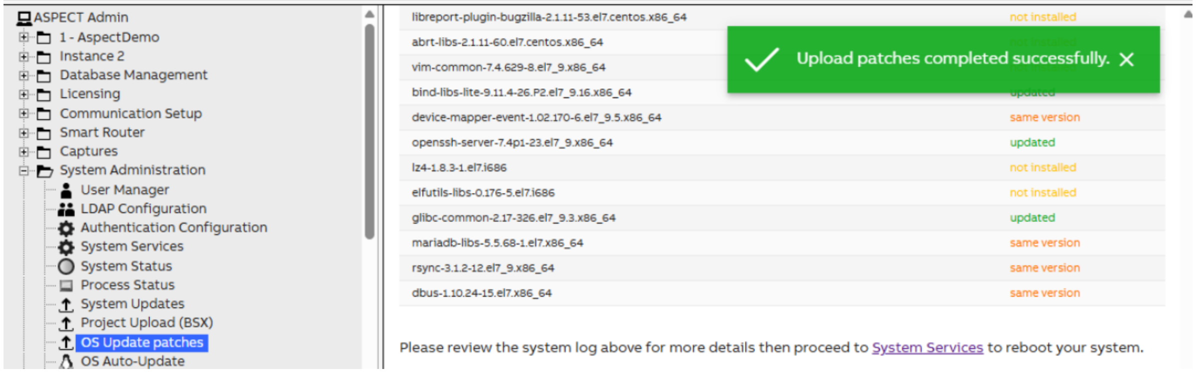
ABB will be providing OS patches and possibly dependency patches in the form of a collection of *.rpm files in a zip archive.

Max file size 500 MB

Install OS patches:

aspect_centos7_EOL_upgrade_v3.08.04.zip 362.602 MB

Please note there are many patches available in the EOL upgrade bundle so the upgrade may take several minutes to finish. Upon successful completion of the EOL upgrade the following screen is displayed:



```
libreport-plugin-bugzilla-2.1.11-53.el7.centos.x86_64      not installed
abrt-libs-2.1.11-60.el7.centos.x86_64
vim-common-7.4.629-8.el7_9.x86_64
bind-libs-lite-9.11.4-26.P2.el7_9.16.x86_64                updated
device-mapper-event-1.02.170-6.el7_9.5.x86_64              same version
openssh-server-7.4p1-23.el7_9.x86_64                       updated
lz4-1.8.3-1.el7.i686                                       not installed
elfutils-libs-0.176-5.el7.i686                             not installed
glibc-common-2.17-326.el7_9.3.x86_64                       updated
mariadb-libs-5.5.68-1.el7.x86_64                           same version
rsync-3.1.2-12.el7_9.x86_64                                same version
dbus-1.10.24-15.el7.x86_64                                 same version
```

✓ Upload patches completed successfully. ✕

Please review the system log above for more details then proceed to System Services to reboot your system.

Successful EOL Ugrade

The device is now considered upgraded to CentOS 7 End Of Life. The following messages may be displayed on the screen and are considered normal.

- same version - means update already applied
- not installed - means the dependency was never initially installed on this device so there is no need to update.

Reboot the server from the System Services menu to continue.

Note: It is possible that you will get an error or the upgrade may appear to be stalled if there are any patches to the Apache Web Server or dependencies since the upgrade depends on the web server to run. If this happens simply rerun the upgrade.

Off-Line CentOS 7 After End Of Life (AEOL) Patches

ABB has partnered with a third party resource to provide important core OS patches for CentOS 7 since it has entered End Of Life status. Patches on core OS packages that rank a CVSS score of 7 or greater will be provided to customers on a quarterly basis from the security patch provider and are downloadable from the ABB Toolbox.

Download the CentOS Patch Bundle for Q1 created March 31, 2025:

- aspect_centos7_OS_patch_v3.08.04-Q1-20250331.bundle.zip

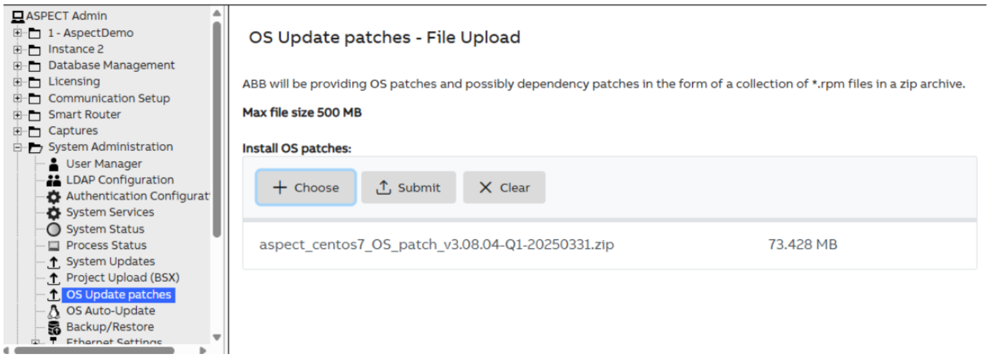
This bundle includes core operating system patches issued from July 1, 2024 until March 31, 2025

Unzip the upgrade bundle to extract the following files

- aspect_centos7_OS_patch_v3.08.04-Q1-20250331.zip
- aspect_centos7_OS_patch_v3.08.04-Q1-20250331.zip.sha256

Verify the integrity of the upgrade bundle by comparing the sha256 hash with the value in the *.sha256 file.

Finally, upload and run the AEOL patch bundle from the OS Update patches menu option in the ASPECT WebUI.



OS Update patches - File Upload

ABB will be providing OS patches and possibly dependency patches in the form of a collection of *.rpm files in a zip archive.

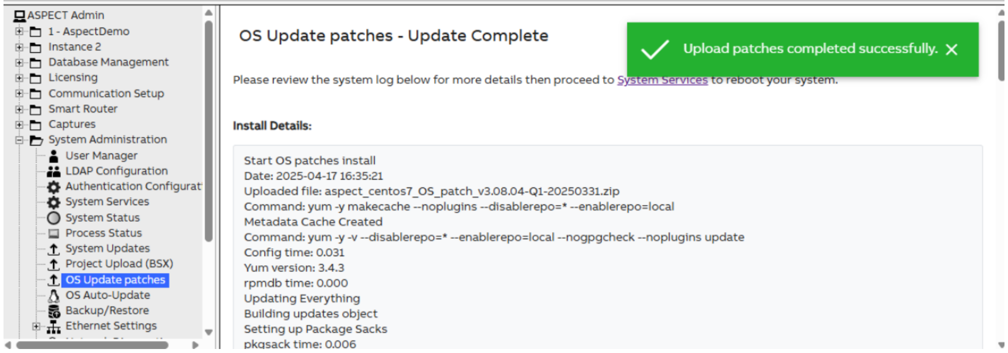
Max file size 500 MB

Install OS patches:

aspect_centos7_OS_patch_v3.08.04-Q1-20250331.zip 73.428 MB

Select CentOS 7 patch bundle and Submit

Please note there are many patches available in the CentOS 7 patch file so it may take several minutes to finish. Upon successful completion of the CentOS 7 patch application the following screen is displayed:



OS Update patches - Update Complete

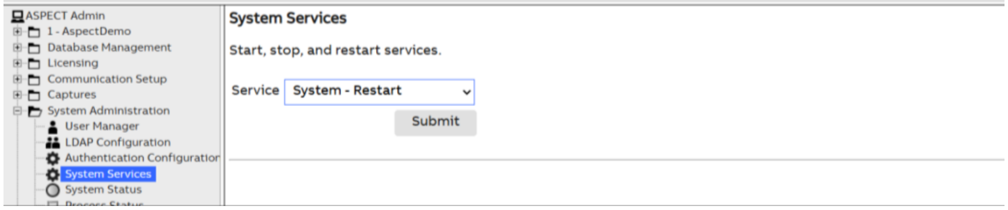
Upload patches completed successfully. ✕

Please review the system log below for more details then proceed to System Services to reboot your system.

Install Details:

```
Start OS patches install
Date: 2025-04-17 16:35:21
Uploaded file: aspect_centos7_OS_patch_v3.08.04-Q1-20250331.zip
Command: yum -y makecache --noplugins --disablerepo=* --enablerepo=local
Metadata Cache Created
Command: yum -y -v --disablerepo=* --enablerepo=local --nogpgcheck --noplugins update
Config time: 0.031
Yum version: 3.4.3
rpmdb time: 0.000
Updating Everything
Building updates object
Setting up Package Sacks
pkgsack time: 0.006
```

Once patch bundles have been applied, restart the system



System Services

Start, stop, and restart services.

Service: System - Restart

After EOL Patch List for CentOS 7

Below is the list of patches that are included in the "after EOL" patch upgrade bundle for Aspect CentOS 7 devices. These are the patches that have been made by ABB's security patch partner to address CVE vulnerabilities with a severity score greater than CVSS score 7 i.e. vulnerabilities of high concern for the CentOS 7 operating system.

The list below summarizes what is included in the following patch bundle released for Q1 2025:

```
aspect_centos7_OS_patch_v3.08.04-Q1-20250331.zip
```

March 2025

- libssh2-1.8.0-4_ol001.el7_9.1 Build Date: Fri 28 Mar 2025 02:28:59 PM UTC - Backported patch to fix **CVE-2023-48795**
- gnutls-3.3.29-9_ol001.el7_6 Build Date: Wed 26 Mar 2025 07:09:53 PM UTC - Backported patches for **CVE-2023-5981, CVE-2024-0553**, and **CVE-2018-16868**
- nettle-2.7.1-9_ol001.el7_9 Build Date: Wed 26 Mar 2025 06:28:21 PM UTC - Backported patches for **CVE-2018-16869**
- bind-9.11.4-26.P2_ol003.el7_9.16 Build Date: Mon 24 Mar 2025 04:09:09 PM UTC - Backported patches to fix **CVE-2022-3094**
- ntp-4.2.6p5-29_ol001.el7.2 Build Date: Wed 19 Mar 2025 08:43:29 PM UTC - Added a warning message that shows the mitigation for **CVE-2019-11331**
- glibc-2.17-326_ol008.el7_9.3 Build Date: Mon 25 Nov 2024 04:30:18 PM UTC - Backported patch to address **CVE-2020-1752**

February 2025

- openssh-7.4p1-23_ol005.el7 Build Date: Tue 11 Feb 2025 04:10:21 PM UTC - Changed **CVE-2023-51385** behavior from automatic disabling of SCP to notification.

January 2025

- rsync-3.1.2-12_ol001.el7_9 Build Date: Thu 30 Jan 2025 01:43:31 PM UTC - Backported patch to address **CVE-2024-12085.**
- krb5-1.15.1-55_ol002.el7_9 Build Date: Wed 29 Jan 2025 07:49:11 PM UTC - Backported fix for **CVE-2024-3596**.
- openssl-1.0.2k-26_ol001.el7_9 Build Date: Mon 13 Jan 2025 09:07:25 PM UTC - Backported patch to address **CVE-2022-2068**.
- httpd-2.4.6-99_ol007.el7.1 Build Date: Mon 13 Jan 2025 07:00:39 PM UTC - Backported patch to address **CVE-2024-38473**.
- openssh-7.4p1-23_ol004.el7 Build Date: Mon 13 Jan 2025 02:00:39 PM UTC - Backported patch to address **CVE-2023-51385**. - Backported patch to address **CVE-2020-15778**.
- python3-setuptools-39.2.0-10_ol001.el7 Build Date: Wed 08 Jan 2025 06:15:15 PM UTC - Backported patch to address **CVE-2024-6345**.
- libarchive-3.1.2-14_ol002.el7 Build Date: Wed 08 Jan 2025 06:01:18 PM UTC - Backported patch to address **CVE-2022-36227**.

December 2024

- python-setuptools-0.9.8-7_ol001.el7 Build Date: Tue 17 Dec 2024 08:34:49 PM UTC - Backported patch for **CVE-2024-6345**.
- glib2-2.56.1-9_ol001.el7 Build Date: Mon 16 Dec 2024 05:44:41 PM UTC - Backported patch to fix **CVE-2019-13012**.
- bind-dyndb-ldap-11.1-7_ol001.el7_9.1 Build Date: Tue 10 Dec 2024 07:22:32 PM UTC - Rebuilt bind-dyndb-ldap against bind-9.11.4-26.P2.el7_9.16 to resolve named-pkcs11 crashes (reported in FreeIPA) after updating to bind > 9.11.4-26.P2.el7_9.15. This issue was introduced by Red Hat around June 12, 2024, and not resolved prior to CentOS 7 going EoL.
  krb5-1.15.1-55_ol001.el7 Build Date: Fri 06 Dec 2024 03:11:58 PM UTC - Backported fix for **CVE-2024-37370**.
- python-2.7.5-94_ol005.el7 Build Date: Thu 05 Dec 2024 02:13:13 PM UTC - Backported patch to address **CVE-2020-27619**.
- tcpdump-4.9.2-4_ol001.el7.1 Build Date: Mon 02 Dec 2024 08:55:40 PM UTC - Backported patch to address **CVE-2020-8037**.
- bind-9.11.4-26.P2_ol002.el7_9.16ofc la Build Date: Mon 02 Dec 2024 08:55:42 PM UTC - Backported patches to address **CVE-2024-1737**.

November 2024

- glibc-2.17-326_ol008.el7_9.3 Build Date: Mon 25 Nov 2024 04:30:18 PM UTC - Backported patch to address **CVE-2020-1752**.
- python-2.7.5-94_ol004.el7 Build Date: Fri 22 Nov 2024 05:48:11 PM UTC - Backported patch to address **CVE-2022-48565**.
- glibc-2.17-326_ol007.el7_9.3 Build Date: Thu 21 Nov 2024 02:00:20 PM UTC - Backported patch to fix **CVE-2017-8804**.
- bind-9.11.4-26.P2_ol001.el7_9.16 Build Date: Wed 20 Nov 2024 05:20:29 PM UTC - Backported patch to fix **CVE-2024-1975**.
- python-2.7.5-94_ol003.el7 Build Date: Mon 18 Nov 2024 07:23:16 PM UTC - Backported patch to address **CVE-2022-45061**.
- glibc-2.17-326_ol006.el7_9.3 Build Date: Fri 15 Nov 2024 03:31:50 PM UTC - Backported patch to fix **CVE-2021-3999**.
- python-urllib3-1.10.2-7_ol001.el7 Build Date: Tue 12 Nov 2024 08:26:47 PM UTC - Backported patches to fix **CVE-2023-43804** and **CVE-2024-37891**.
- glibc-2.17-326_ol005.el7_9.3 Build Date: Tue 12 Nov 2024 07:44:50 PM UTC - Backported patch to address **CVE-2023-4806**, thus preventing **CVE-2023-5156**.
- systemd-219-78_ol004.el7.9 Build Date: Mon 11 Nov 2024 10:05:09 PM UTC - Reworked the backport of the patch to address **CVE-2018-6954**.
- perl-5.16.3-299_ol002.el7 Build Date: Mon 11 Nov 2024 03:43:48 PM UTC - Backported patch to fix **CVE-2020-16156**.
- bash-4.2.46-35_ol002.el7 Build Date: Thu 07 Nov 2024 08:31:51 PM UTC - Patch to fix **CVE-2012-6711**.
- httpd-2.4.6-99_ol006.el7.1 Build Date: Thu 07 Nov 2024 04:53:11 PM UTC - Backported patch to fix **CVE-2024-24795**.
- systemd-219-78_ol003.el7.9 Build Date: Wed 06 Nov 2024 10:38:26 PM UTC - Reverted patches that addressed **CVE-2018-6954** due to an issue with chrony.
- systemd-219-78_ol002.el7.9 Build Date: Mon 04 Nov 2024 07:46:19 PM UTC - Backported patch to address **CVE-2018-6954**.

October 2024

- gcc-4.8.5-44_ol001.el7 Build Date: Thu 31 Oct 2024 06:06:00 PM UTC - Backported patch to fix **CVE-2021-37322**.
- glibc-2.17-326_ol004.el7_9.3 Build Date: Thu 31 Oct 2024 02:12:52 PM UTC - Backported patch to fix **CVE-2022-23218**.
- bash-4.2.46-35_ol001.el7 Build Date: Wed 30 Oct 2024 07:12:13 PM UTC - Backported patch for **CVE-2019-18276**.
- glibc-2.17-326_ol003.el7_9.3 Build Date: Tue 29 Oct 2024 05:22:58 PM UTC - Backported patch to fix **CVE-2022-23219**.
- perl-5.16.3-299_ol001.el7 Build Date: Tue 29 Oct 2024 01:45:21 PM UTC - Backported patch to fix **CVE-2016-6185**. - Backported patch to fix **CVE-2023-31484**.
- python3-3.6.8-21_ol004.el7_9 Build Date: Tue 29 Oct 2024 02:38:30 PM UTC - Backported patch to address **CVE-2020-10735**.
- python-2.7.5-94_ol002.el7 Build Date: Mon 28 Oct 2024 02:20:42 PM UTC - Backported patch to address **CVE-2022-48560**. - Backported patch to address **CVE-2020-10735**.
- python3-3.6.8-21_ol003.el7_9 Build Date: Thu 24 Oct 2024 07:33:30 PM UTC - Applied patch to address **CVE-2022-48560**. - Applied patch to address **CVE-2020-27619**.
- binutils-2.27-44.base_ol001.el7.1 Build Date: Wed 23 Oct 2024 07:11:24 PM UTC - Backported patch to address **CVE-2022-44840**. - Backported patch to address **CVE-2021-37322**. - Backported patch to address **CVE-2021-45078**.
- systemd-219-78_ol001.el7.9 Build Date: Fri 18 Oct 2024 04:09:10 PM UTC - Backported patch to address **CVE-2023-26604**.
- python3-3.6.8-21_ol002.el7_9 Build Date: Thu 17 Oct 2024 09:17:34 PM UTC - Backported patch to address **CVE-2022-48565**.
- perl-HTTP-Tiny-0.033-3_ol001.el7 Build Date: Tue 15 Oct 2024 02:04:43 PM UTC - Applied patch to address **CVE-2023-31486**.
- httpd-2.4.6-99_ol005.el7.1 Build Date: Mon 14 Oct 2024 01:37:56 PM UTC - Backported patch to fix **CVE-2022-28614**. - Backported patch to fix **CVE-2022-28615**.
- glibc-2.17-326_ol002.el7_9.3 Build Date: Thu 10 Oct 2024 01:00:27 PM UTC - Backported patch to mitigate **CVE-2021-35942**.
- python-2.7.5-94_ol001.el7 Build Date: Mon 07 Oct 2024 04:09:43 PM UTC - Backported patch to address **CVE-2017-1000158**.

September 2024

- httpd-2.4.6-99_ol004.el7.1 Build Date: Mon 30 Sep 2024 01:53:43 PM UTC - Backported patches to fix **CVE-2022-29404** and **CVE-2024-38476**.
- httpd-2.4.6-99_ol003.el7.1 Build Date: Thu 26 Sep 2024 06:57:09 PM UTC - Backported patch to address **CVE-2024-38474**. - Backported patch to address **CVE-2024-38475**. - Backported patch to address **CVE-2024-39573**.
- wget-1.14-18_ol001.el7.1 Build Date: Tue 17 Sep 2024 05:49:16 PM UTC - Backported patch to fix **CVE-2024-38428**.
- httpd-2.4.6-99_ol002.el7.1 Build Date: Wed 11 Sep 2024 01:39:51 PM UTC - Backported patch to address **CVE-2024-38477**.
- turbojpeg-1.2.90-8_ol001.el7 Build Date: Mon 09 Sep 2024 06:43:37 PM UTC - Backported patch to fix **CVE-2019-2201**.

August 2024

- openssh-7.4p1-23_ol002.el7 Build Date: Thu 15 Aug 2024 03:45:39 PM UTC - Fixed multiple vulnerabilities: **CVE-2019-6109**, **CVE-2019-6110**, and **CVE-2019-6111**.
- httpd-2.4.6-99_ol001.el7.1 Build Date: Fri 09 Aug 2024 08:44:43 PM UTC - Backported patch to fix HTTP response splitting for **CVE-2023-38709**.

July 2024

- libarchive-3.1.2-14_ol001.el7 Build Date: Mon 29 Jul 2024 09:05:17 PM UTC - Backported patch to fix improper link resolution vulnerability **CVE-2021-31566**.
- openssh-7.4p1-23_ol001.el7 Build Date: Tue 30 Jul 2024 08:11:28 PM UTC - Backported patch to address **CVE-2018-20685**.
- sqlite-3.7.17-8_ol001.el7.1 Build Date: Tue 30 Jul 2024 04:03:11 PM UTC - Backported heap out-of-bound read fix for **CVE-2019-8457**.
- libtirpc-0.2.4-0.16_ol001.el7 Build Date: Fri 26 Jul 2024 09:13:41 PM UTC - Backported DoS vulnerability fix for **CVE-2021-46828**.
- glibc-2.17-326_ol001.el7_9.3 Build Date: Mon 08 Jul 2024 01:00:26 PM UTC - Applied OpenLogic patch from glibc-2.17-326_ol001 to latest CentOS 7 version at EoL (glibc-2.17-326.3) for **CVE-2009-5155.**
- python3-3.6.8-21_ol001.el7_9 Build Date: Mon 08 Jul 2024 02:18:05 PM UTC - Applied OpenLogic patch from python36-3.6.8-19_ol001 to latest CentOS 7 version at EoL (python36-3.6.8-21) for **CVE-2022-45061**.

GENERAL USABILITY IMPROVEMENTS

ASP-5497	Restrict special characters in graphic import file name to preserve graphics links on Graphics (CCB)
ASP-6755	ASPECT PostPushService Element cannot be triggered (CCB)
ASP-7023	eMap writes do not work if user/pass combination is not the same between ENT and satellite devices (CCB)
ASP-7303	French translation cleanup in ASPECT (CCB)
ASP-7445	Set Time function is not working if NTP is disabled on Matrix-2 (CCB)
ASP-7446	Set NTP Servers does not work correctly
ASP-7464	SSO (remote graphics links auto-login) not working on some targets in 3.08.03 (CCB)
ASP-7473	"Import Map from Target" not working in `3.08.03` (CCB)
ASP-7507	Add ngAdmin Romanian localizations to ASPECT
ASP-7571	Remove misleading Gmail OAuth2 instructions from emailers in ASPECT
ASP-7523	Users and Groups: If more than one user is deleted, one of them is still displayed as part of a group
ASP-7577	eMap Remote trends and not working if username/passwords are not synchronized
ASP-7592	Setting ngAdmin login group(s) ("Groups-ngAdmin" in Security Subsystem) causes eMap to break

SECURITY IMPROVEMENTS

Note: **There will be a Vendor Security Advisory published for the vulnerabilities patched in this release. All ABB Product Advisories can be found here: ABB Cyber security alerts and notifications**

ASP-7027	Add option to the WebUI to allow OS patches to be applied (CentOS EOL/Security Patches)
ASP-7142	Secure CVE patches for Apache `2.4.6` to mitigate CVE-2024-40725 and CVE-2024-39884
ASP-7143	Secure CVE Patches for MariaDb `5.5.68` to mitigate CVE-2022-27448, CVE-2022-27449 and CVE-2022-27452
ASP-7146	Upgrade Java to OpenJDK `8.0.412` to mitigate CVE-2024-20932 and CVE-2024-20918
ASP-7224	ABB Cylon Aspect Remote Guest2Root Exploit Authenticated - PHP version
ASP-7226	Further harden YUM lookup script per researcher suggestions
ASP-7238	Insecure session management authorization bypass
ASP-7239	Authorized RCE on MIX.log download
ASP-7247	Remote Guest2Root Exploit Authenticated - nodejs version
ASP-7293	Unify password rules across the 4 places where you can change passwords
ASP-7294	Create "after EOL" security patch bundle(s) for CentOS 7
ASP-7297	Add a new menu option on CentOS 7 target to allow OS Updates
ASP-7317	Review nodejs codebase for security vulnerabilities and remediate
ASP-7444	Nodejs - Security: IP Port Administration - Save data
ASP-7466	ABB Cylon ASPECT `3.08.03` (CookieDB) SQL Injection
ASP-7475	Review Servlets for Command Injection Vulnerabilities
ASP-7476	Review Servlets for SQL Injection vulnerabilities
ASP-7477	Review Servlets for Relative Path Traversal vulnerabilities
ASP-7478	Review UserManager.java for an unchecked loop condition
ASP-7513	Secure CVE Patches for sudo 1.8.23 CVE-2023-22809.
ASP-7565	Create Offline CentOS 7 End Of Life upgrade bundle

Customer Impact

Users **must upgrade as soon as possible** to ensure their ASPECT targets are secure and to take advantage of the latest features and improvements.

Note:	ASPECT v`3.08.04` is an irrevocable upgrade meaning if an ASPECT target has been upgraded to `v3.08.04` it cannot be backed down to any pre-v`3.08.04` release.

Note	ASPECT is not designed to be an “internet-facing” server application. If you need to access the ASPECT device remotely, you should do so through a secure VPN (and not a publicly accessible internet domain).

Note:	ABB recommends that all unnecessary ports are closed on an ASPECT device. After upgrading, always review port configuration (WebUI > Communication Setup > IP Port Administration) for any unnecessarily open ports and close accordingly.

Note:	It is recommended that `.aam` file checksums are verified against those published on the online ToolBox before a System Upgrade is performed.

Note:	If you have any difficulty accessing ASPECT after upgrade, you may need to: 1. Clear your browsers history/cookies and restart the browser to clear out the older version/data (performing a hard refresh with Ctrl+F5 is an alternative option). 2. If login is still not working after clearing the cache, you may need to use the alternative WebUI login page at `https://192.168.0.1/altlogin.php` (replace the IP with your device’s host/IP).