Windows 10 End of Life (EOL)

The IATA CUSS and CUPPS Task Forces reporting to the Customer Journey Delivery Working Group met in Montreal in May 2025 and agreed that, as of January 1, 2026, IATA-recognized common use standards (CUPPS, CUSS, SBD) used for passenger processing are not designed to be supported on End of Life Windows operating systems.

Background

When Windows 10 was released on July 29, 2015, Microsoft made a commitment to provide 10 years of product support. Effective October 14, 2025, Microsoft discontinued its support for Windows 10 Home and Pro. This means that Microsoft no longer provides technical assistance or security updates for Windows 10, which are essential to help protect systems from emerging security threats.

Existing LTSC (Long-Term Servicing Channel) releases will continue to receive updates beyond October 14, 2025 based on their lifecycles:

- Windows 10 Enterprise LTSC 2019: Extended support ends January 9, 2029.
- Windows 10 Enterprise LTSC 2021: Extended support ends January 13, 2032.

Microsoft strongly recommends that all users and organizations running Windows 10 migrate to a supported version, such as Windows 11 or supported LTSC editions of Windows 10 (listed above). To avoid potential disruptions and security vulnerabilities, the migration should be completed well before the end-of-support date. For more details, refer to Microsoft documentation on Windows 10 End of Support.

Risks of Continued Use of Windows 10 Beyond Support

Hardware Incompatibility

Intel has discontinued several older generations of chips originally compatible with Windows 10. As a result, PC manufacturers have shifted focus entirely to devices compatible with Windows 11 or supported LTSC (Long-Term Servicing Channel) versions of Windows 10 (such as Windows 10 Enterprise LTSC 2019 or Windows 10 IoT Enterprise LTSC 2021). This means that replacing or scaling up installations operating on Windows 10 is becoming increasingly difficult, as compatible hardware is no longer produced or supported.

Software and driver providers incompatibility

Providers of software and drivers focus on Windows 11 operating system versions and their specific APIs. Providers of software components and drivers enhance their products regarding the operating system functionalities. That means that software or drivers on unsupported systems may only work with limited functionality or not at all.

Compliance and Legal Risk

Incidents of data breaches, identity theft, and financial fraud are now common across industries. Airports, airlines, and their partners have all been targets, with breaches impacting hundreds of millions of individuals. The consequences include significant financial losses, reputational damage, and regulatory penalties, especially under legislation such as the General Data Protection Regulation (GDPR). Unsupported operating

systems heighten the risk of such incidents due to a lack of security updates, and they may prevent implementations from being compliant with cybersecurity rules (i.e., NIS2).

Payment Card Industry Data Security Standard (PCI DSS)

- PCI DSS mandates that all systems handling payment data must maintain high levels of security. This includes operating systems receiving regular security patches, as outlined in the PCI DSS Quick Reference Guide v3.2.1.

- Systems used in airport environments — including CUSS and Self Bag Drop (SBD) devices — are increasingly used for payment transactions . This elevates risk exposure when these systems run unsupported or unpatched software.

Impact

- **Continued use of Windows 10 beyond October 14, 2025, exposes all stakeholders — passengers, airlines, and airports — to security vulnerabilities**, including data breaches, identity theft, and financial loss, in addition to potential non-compliance with GDPR and PCI DSS, resulting in fines and reputational harm.

- **Airports and airlines may fail to meet the latest PCI DSS Requirement, and NIS2**, which requires the timely application of security patches — unavailable once Windows 10 reaches the end of support.

- **Declining Application Support**
  Over time, a significant number of third parties, such as application providers, airlines, and their DCS providers, may no longer develop nor support applications for Windows 10 environments.

Action Required

It is of paramount importance that all parties (Airlines, Airports, & Platform providers) create and follow a plan to migrate systems from Windows 10 to Windows 11 or supported LTSC versions of Windows 10 to reduce the risks and costs of security breaches and operational integrity that can occur when Windows 10 and other third-party applications are EOL.

- **Airports:**

  - Meet with your common use provider to agree on a migration plan, which may include new hardware, as part of your contractual obligations.

  - Plan to migrate from Windows 10 to Windows 11 or supported LTSC (Long-Term Servicing Channel) versions of Windows 10 (such as Windows 10 Enterprise LTSC 2019 or Windows 10 IoT Enterprise LTSC 2021) on all workstations and kiosks.

  - Meet with the operating airlines to set dates. Verify with the airlines when their applications will be compliant with the required operating systems.

- **Airlines:**
  - Ensure your applications, whether developed in-house or externally, are ready for deployment on Windows 11 or supported LTSC (Long-Term Servicing Channel) versions of Windows 10 (such as Windows 10 Enterprise LTSC 2019 or Windows 10 IoT Enterprise LTSC 2021).
  - Ensure the application has no reliance on 16-bit processes or executables. Current available workstations are 64-bit.
- **Platform providers:**
  - Ensure that your platform functions as desired on Windows 10 LTSC options and Windows 11
  - Work with Airlines during application certification/integration to ensure no impact as airports transition to Windows 10 LTSC or Windows 11 operating systems