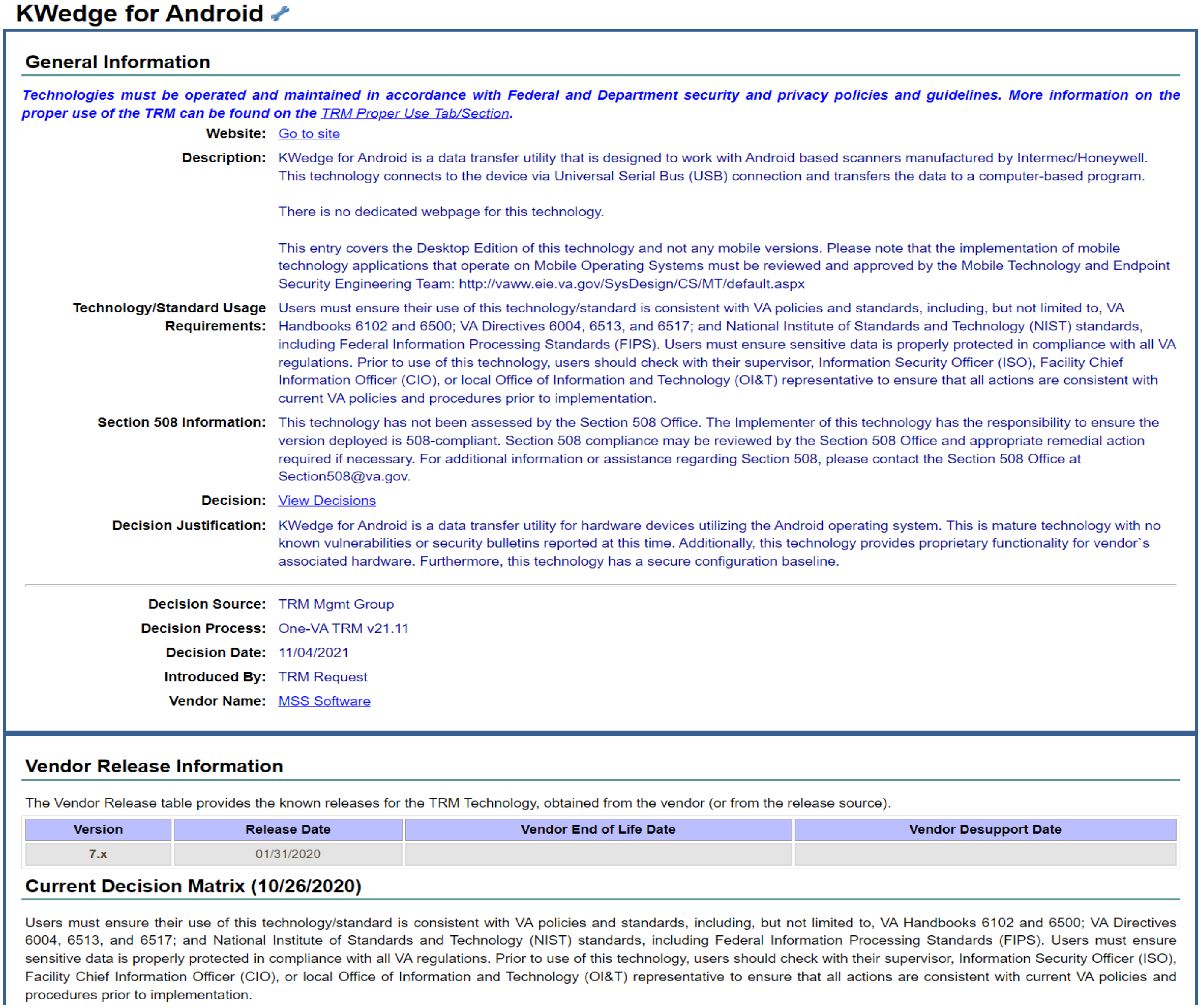
KWedge for Android

Reference: VA Technical Reference Manual (TRM) v 22.8 [VA Intranet: KWedge for Android (va.gov)]



KWedge for Android

General Information

Technologies must be operated and maintained in accordance with Federal and Department security and privacy policies and guidelines. More information on the proper use of the TRM can be found on the TRM Proper Use Tab/Section.

Website:	Go to site
Description:	KWedge for Android is a data transfer utility that is designed to work with Android based scanners manufactured by Intermec/Honeywell. This technology connects to the device via Universal Serial Bus (USB) connection and transfers the data to a computer-based program. There is no dedicated webpage for this technology. This entry covers the Desktop Edition of this technology and not any mobile versions. Please note that the implementation of mobile technology applications that operate on Mobile Operating Systems must be reviewed and approved by the Mobile Technology and Endpoint Security Engineering Team: http://vaww.eie.va.gov/SysDesign/CS/MT/default.aspx
Technology/Standard Usage Requirements:	Users must ensure their use of this technology/standard is consistent with VA policies and standards, including, but not limited to, VA Handbooks 6102 and 6500; VA Directives 6004, 6513, and 6517; and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards (FIPS). Users must ensure sensitive data is properly protected in compliance with all VA regulations. Prior to use of this technology, users should check with their supervisor, Information Security Officer (ISO), Facility Chief Information Officer (CIO), or local Office of Information and Technology (OI&T) representative to ensure that all actions are consistent with current VA policies and procedures prior to implementation.
Section 508 Information:	This technology has not been assessed by the Section 508 Office. The Implementer of this technology has the responsibility to ensure the version deployed is 508-compliant. Section 508 compliance may be reviewed by the Section 508 Office and appropriate remedial action required if necessary. For additional information or assistance regarding Section 508, please contact the Section 508 Office at Section508@va.gov.
Decision:	View Decisions
Decision Justification:	KWedge for Android is a data transfer utility for hardware devices utilizing the Android operating system. This is mature technology with no known vulnerabilities or security bulletins reported at this time. Additionally, this technology provides proprietary functionality for vendor`s associated hardware. Furthermore, this technology has a secure configuration baseline.
Decision Source:	TRM Mgmt Group
Decision Process:	One-VA TRM v21.11
Decision Date:	11/04/2021
Introduced By:	TRM Request
Vendor Name:	MSS Software

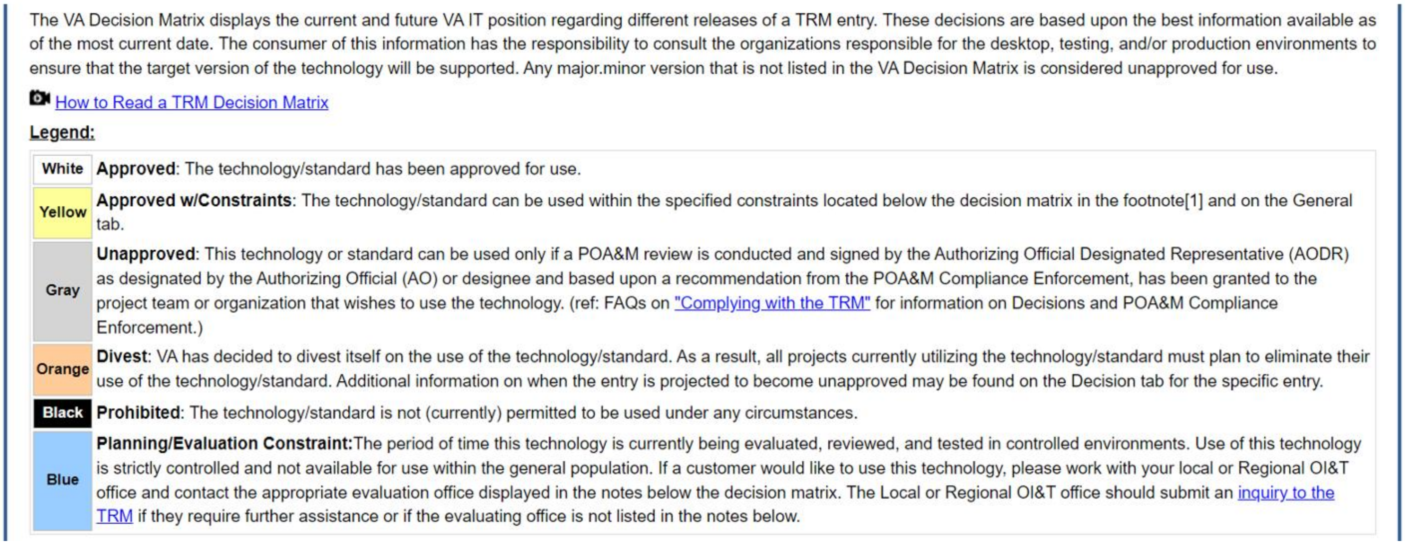
Vendor Release Information

The Vendor Release table provides the known releases for the TRM Technology, obtained from the vendor (or from the release source).

Version	Release Date	Vendor End of Life Date	Vendor Desupport Date
7.x	01/31/2020		

Current Decision Matrix (10/26/2020)

Users must ensure their use of this technology/standard is consistent with VA policies and standards, including, but not limited to, VA Handbooks 6102 and 6500; VA Directives 6004, 6513, and 6517; and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards (FIPS). Users must ensure sensitive data is properly protected in compliance with all VA regulations. Prior to use of this technology, users should check with their supervisor, Information Security Officer (ISO), Facility Chief Information Officer (CIO), or local Office of Information and Technology (OI&T) representative to ensure that all actions are consistent with current VA policies and procedures prior to implementation.



The VA Decision Matrix displays the current and future VA IT position regarding different releases of a TRM entry. These decisions are based upon the best information available as of the most current date. The consumer of this information has the responsibility to consult the organizations responsible for the desktop, testing, and/or production environments to ensure that the target version of the technology will be supported. Any major.minor version that is not listed in the VA Decision Matrix is considered unapproved for use.

How to Read a TRM Decision Matrix

Legend:

White	**Approved**: The technology/standard has been approved for use.
Yellow	**Approved w/Constraints**: The technology/standard can be used within the specified constraints located below the decision matrix in the footnote[1] and on the General tab.
Gray	**Unapproved**: This technology or standard can be used only if a POA&M review is conducted and signed by the Authorizing Official Designated Representative (AODR) as designated by the Authorizing Official (AO) or designee and based upon a recommendation from the POA&M Compliance Enforcement, has been granted to the project team or organization that wishes to use the technology. (ref: FAQs on "Complying with the TRM" for information on Decisions and POA&M Compliance Enforcement.)
Orange	**Divest**: VA has decided to divest itself on the use of the technology/standard. As a result, all projects currently utilizing the technology/standard must plan to eliminate their use of the technology/standard. Additional information on when the entry is projected to become unapproved may be found on the Decision tab for the specific entry.
Black	**Prohibited**: The technology/standard is not (currently) permitted to be used under any circumstances.
Blue	**Planning/Evaluation Constraint:**The period of time this technology is currently being evaluated, reviewed, and tested in controlled environments. Use of this technology is strictly controlled and not available for use within the general population. If a customer would like to use this technology, please work with your local or Regional OI&T office and contact the appropriate evaluation office displayed in the notes below the decision matrix. The Local or Regional OI&T office should submit an inquiry to the TRM if they require further assistance or if the evaluating office is not listed in the notes below.

Release/Version Information:

VA decisions for specific versions may include a '.x' wildcard, which denotes a decision that pertains to a range of multiple versions.

For example, a technology approved with a decision for 7.x would cover any version of 7.(Anything) - 7.(Anything). However, a 7.4.x decision would cover any version of 7.4.(Anything), but would not cover any version of 7.5.x or 7.6.x on the TRM.

VA decisions for specific versions may include '+' symbols; which denotes that the decision for the version specified also includes versions greater than what is specified but is not to exceed or affect previous decimal places.

For example, a technology approved with a decision for 12.6.4+ would cover any version that is greater than 12.6.4, but would not exceed the .6 decimal ie: 12.6.401 is ok, 12.6.5 is ok, 12.6.9 is ok, however 12.7.0 or 13.0 is not.

<Past	CY2021				CY2022				CY2023				Future>
Release	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
7.x	Approved w/Constraints [3, 4, 5]	Approved w/Constraints [3, 4, 5]	Approved w/Constraints [3, 4, 5]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	Approved w/Constraints [3, 5, 6, 7]	

Decision Constraints

[1] Per the Initial Product Review, users must abide by the following constraints:

- To be used within VA, the underlying operating system, full disk encryption, or other third-party Federal Information Processing Standards (FIPS) 140-2 validated applications must be leveraged to protect VA sensitive information.

[2] Veterans Affairs (VA) users must ensure VA sensitive data is properly protected in compliance with all VA regulations. All instances of deployment using this technology should be reviewed by the local ISO (Information Security Officer) to ensure compliance with VA Handbook 6500.

[3] Technology must remain patched and operated in accordance with Federal and Department security policies and guidelines in order to mitigate known and future security vulnerabilities.

[4] This technology requires using a Universal Service Bus (USB) technology to transfer data into the records. As such, proper precautions need to be taken to protect data.

Per the Initial Product Review, users must abide by the following constraints:

- To be used within VA, the underlying operating system, full disk encryption, or other third-party Federal Information Processing Standards (FIPS) 140-2 validated applications must be leveraged to protect VA sensitive information.

[5] Veterans Affairs (VA) users must ensure VA sensitive data is properly protected in compliance with all VA regulations. All instances of deployment using this technology should be reviewed by the local ISO (Information Security Officer) to ensure compliance with VA Handbook 6500.

[6] This technology requires using a Universal Service Bus (USB) technology to transfer data into the records. As such, proper precautions need to be taken to protect data. Please see the referenced baseline document for more information.

Per the Initial Product Review, users must abide by the following constraints:

- To be used within VA, the underlying operating system, full disk encryption, or other third-party Federal Information Processing Standards (FIPS) 140-2 validated applications must be leveraged to protect VA sensitive information.

[7] New installations or major expansions of this technology that transmit data over the VA Wide Area Network (WAN) must complete a WAN impact review (yourIT Service Portal:[SNOW Service Requests]) prior to implementation to ensure proper compliance to VA network design and usage requirements.

Note: At the time of writing, version 7.3 is the most current version released.

References

The following reference(s) are associated with this entry:

Type	Name	Source	Description	VA Only
Other VA Analysis	KWedge for Android Initial Product Review (IPR)		This links to the Initial Product Review (IPR) for KWedge for Android.	True
Other VA Analysis	KWedge Android Baseline		This document outlines the baseline configuration of KWedge for Android devices.	True

Correlation

NOTE: Correlation information is only available to authorized users.

Correlated Entry ID
17296

Technology Components

Note: This list may not be complete. No component, listed or unlisted, may be used outside of the technology in which it is released. The usage decision for a component is found in the Decision and Decision Constraints.

Name	Description
No components have been identified for this entry.	

Technology Licensing

Software Enterprise License Agreements (ELAs) are negotiated based on software requirements gathered from the VA user community and valid for a specific Period of Performance (POP). The "VA License Contact information" section identifies who you should contact to understand the software ELAsspecific "Terms and Conditions (T&Cs)". The Vendor License Usage Information section directs the user to the vendor licensing methodology for the specific software.

The VA user community must adhere to the terms and conditions by communicating with key stakeholders (eg., Contract Officer Representative), analyzing project specific requirements, mapping project requirements and project timelines against the software ELAsbefore installing of software product instances.

VA License Contact Information:

License Environment	Organization Name	Contact	License Expiration Date
Commercial Licenses may be available, but the VA license contact information is not available.			

Vendor License Usage Information:

License Environment	License Name	License Agreement
All	Commercial License	Not Provided

VA Categories

How to Browse Comparable Technologies

Domain Area	Category	Customer Guidance	Category Locked By ELT Date
Systems Management Systems Management Tools	Asset Management		

Operating Systems Supported by the Technology

- Windows Client - Approved w/Constraints

Technologies/Standards Relationships

Runtime Dependencies:

- No runtime dependencies have been identified.

Comparable Technologies:

- No comparable entries have been identified.

Companion Technologies/Supported Standards:

- No companion technologies/standards have been identified.

Update Request Summary

Name:	KWedge for Android
Update Detail:	A new baseline for this technology has been ratified. Please ensure that the baseline is referenced and that only versions approved by the baseline are approved in TRM. Older versions should be divested for a short period and then unapproved. Good morning, EBSR22-2200, Barcode Scanners with KWedge for Android Enterprise Implementation Standard, is complete. The attached standard is now ratified. I have created the following Change Request in Service Now to publish this standard on the BCM SharePoint Portal: CHG0230445. Please let me know if you have any questions. Thank you, Jessica
Date Requested:	10/27/2021
Status:	Resolved
Status Date:	11/04/2021
VA Category:	This request has not been classified.

All Requests and Inquiries

Date	Type	Title	Status
12/17/2021	Update	KWedge for Android	Rejected
12/16/2021	Update	KWedge for Android	Rejected
11/05/2021	Update	KWedge for Android	Rejected
10/27/2021	Update	KWedge for Android	Resolved
10/26/2021	Inquiry	The Barcode Scanners with KWedge for Android Site Implementation Stand	Resolved
10/26/2020	Update	KWedge for Android	Resolved
01/22/2020	Add	KWedge for Android Devices	Resolved

General Analysis

Adoption Benefits

- At the time of writing, no National Institute of Standards and Technology (NIST) vulnerabilities had been reported and no VA Network Security Operations Center (NSOC) bulletins had been issued for the latest versions of this technology.
- This technology provides proprietary functionality for vendor`s associated hardware.
- This is a mature technology.

Adoption Risks

- The vendor cannot provide a FIPS 140-2 certificate of compliance; therefore, connectivity to VA wireless networks cannot be recommended at this time. Therefore, the only remaining option compatible with KWedge for Android is to use a Universal Serial Bus (USB) connection. Proper security precautions must be taken when USB connections are utilized.
- This technology can potentially transmit data over the VA Wide Area Network (WAN).
- The potential exists to store Personally Identifiable Information (PII), Protected Health Information (PHI) and/or VA Sensitive data and proper security standards must be followed in these cases.
- Due to the rapid release schedule of this technology, the VA may be unable to update to the most recent patch and may require a deployment model requiring the use of specific versions.
- There is limited publicly available technical documentation for this technology.

Architectural Benefits

- This technology has a secure configuration baseline.

Architectural Risks

- This technology is not portable as it runs only on Windows platforms.

- The information contained on this page is accurate as of the Decision Date (11/04/2021).

Printed Date: 8/30/2022 12:58:35 PM