HALOCAD

Frequently Asked Questions

Welcome to HALOCAD FAQ. In this document, you will find answers to important questions regarding HALOCAD products, services, security, and infrastructure policies.

The purpose of this document is to provide quick guide to the frequently asked questions about our HALAOCAD product.

While this document contains answers to our most frequently answered questions, should you have any additional questions, please contact our sales representative or our support team.

TABLE OF CONTENTS:

GENERAL FAQs

Q: What can the user do with HALOCAD?

A: The user can protect engineering CAD models, drawings, technical documents and enforce data security across its entire life cycle.

Q: What strategic partnerships do you have?

A: We have development partnership with all major CAD/PLM vendors: Autodesk, PTC, Siemens, Bentley Systems.

In addition, we have strategic and development partnership with SAP and Microsoft. We are also member of the MISA (Microsoft Intelligent Security Association) and our product is listed in the SAP and Microsoft Appstore.

Q: Where can we find the FAQs on Azure?

A: The FAQs provided by Microsoft on Azure can be found at the below links.

https://docs.microsoft.com/en-us/azure/information-protection/faqs
https://docs.microsoft.com/en-us/azure/information-protection/faqs-infoprotect
https://docs.microsoft.com/en-us/azure/information-protection/faqs-rms

Q: Who are your reference customers?

1. Leading manufacturer of semiconductor equipment's in Europe
2. Leading healthcare & scientific instrument manufacturer in Americas

Q: What are the commonly used sensitive data in an Engineering/R&D that needs protection?

A: The commonly used sensitive data in an Engineering/R&D are:
1. CAD drawings
2. PLM files
3. Product design
4. Digital drawings/Illustrations
5. Prototypes

Q: What is the prerequisite software for HALOCAD Add-On?

A: Microsoft Information Protection (MIP) or Active Directory Rights Management Service (ADRMS) should be available and active at the customer location.

PRODUCT FAQs

Q: Who can open the encrypted CAD files and documents?

A: Only authorized users who have valid credentials can access the encrypted CAD files and documents.

Q: What exactly happens when an authorized supplier opens the CAD file?

A: When an authorized supplier opens a protected CAD file, then the rights will be enforced based on the configuration provided in the Protection Label such as View, Edit, Print, Copy, Export, and so on.

Q: What can the users do with the opened encrypted document?

A: The user can act upon the document based on one or more of the assigned privileges – view, edit, copy, print, or export.

Q: Is it possible to protect files without end user intervention?

A: Our DRM solution can enforce default label to the new CAD files based on organization policy and end user does not have to do anything.

Q: What are the methods for the user to authenticate and access a protected file and if there is a way to set a re-authentication period?

A: HALOCAD uses the MIP SDK and the Microsoft authentication methods which are integrated there. This also includes the feature of caching the user credentials and triggering the re-authentication based on the period set in the Microsoft AD.

Q: Is it possible to change the label after the CAD file is shared with an authorized supplier?

A: Only “Owner” of the protected file has rights to change the label and republish to the supplier.

Q: How AIP works with taking screen shots?

A: Taking screenshots using Snipping Tool, PrtScr etc. can be prevented by disabling the copy access in the AIP labels.

Q: What happens when an unauthorized user opens an encrypted file?

A: If an unauthorized user tries to open the encrypted file, he will be prompted with an appropriate error message and cannot access the file.

Q: How to protect PDF files, generated from CAD models or drawings?

A: When the user exports a CAD models or drawings into PDF format, our DRM solution encrypts the PDF file with the appropriate label as per organization policy.

Q: Is the protection of CAD files achieved by encryption? Does the file extension change after encryption?

A: Yes, we encrypt the CAD files using MIP SDK. Also, we retain the same file extension after encryption.

Q: Who creates the labels in the background and how it is managed?

A: Azure administrator creates and manages the labels in the background. He can create profile, classification schema, classification rule, and action rule to manage the label assignment to different users in the organization.

Q: How the same drawing can be enabled as view only and modify for different set of users?

A: Each label will have the details of user and corresponding rights in the Azure portal. All the rules to access the appropriate label are managed in the HALOCORE central server..

Q: Is it possible to have a defined period of access for partners? If so, how it works?

A: Currently, MIP label offers the following options for content expiry.
a) On a specific date
b) A number of days after label is applied

Q: How do we track the usage of protected data outside the organization?

A: The tracking of protected CAD files and documents is possible using Azure analytics and audit logs.

Q: Can a non-IT user or Business user (who is new to label administration) manage the centralized policy controls?

A: Microsoft provides a standard guide on how to manage and control the policies in Azure portal and organizations can train their users.

Q: What is HALOCAD Reader?

A: The user in the partner or supplier organization can have “View only” access to the encrypted files if there is no MIP or ADRMS. This is possible using the free standalone Add-on “HALOCAD Reader” to view the file and the reader can be downloaded from Microsoft Appstore.

Q: Are the HALOCAD Add-ons specific to CAD applications?

A: The HALOCAD Add-ons are developed and configured using the CAD specific APIs to make them compatible with the different CAD applications. Hence, we have separate Add-ons for each of the CAD applications – AutoCAD, Inventor, Creo, NX, Solid Edge, or MicroStation.

Q: Is it possible to set an expiry date for a CAD file or document?

A: Our DRM solution enables outsourced data to be access controlled based on a specified duration. The outsourcing manager in the parent organization can enforce data access expiration e.g. 2 weeks for the designated supplier, monitor the progress and extend the access duration as needed.

Q: What happens when an authorized supplier opens the CAD model or drawing after the label expires?

A: The user will get an error message that he or she does not have permission to open this document because it has crossed the expiry date.

Q: Is it possible to provide offline access to a CAD file or document?

A: Our DRM solution enables data access definition when there is no internet or network connection through appropriate rule definitions in the Microsoft Azure layer.

Q: What if the available sensitivity labels in the HALOCAD dropdown are not appropriate for the drawing I am working on?

A: Contact your MIP administrator and request a modification or a new label. See Learn about sensitivity labels - Microsoft 365 Compliance | Microsoft Docs.

Q: Who decides what labels should be used for various CAD drawings?

A: Usually this is decided by the engineering managers. The labels provided by MIP for office documents (Confidential, Top Secret, General, Read Only) may be adequate. Engineering projects might need their own specific labels.

Q: Can I create my own sensitivity labels?

A: No, at this time, the sensitivity labels for HALOCAD are solely managed by MIP.

Q: What if the drawing I am working on has the wrong label?

A: If your sign-on user is the owner of the drawing, you may change it by selecting a new label from the HALOCAD dropdown. If your user is not the owner, you must contact the original owner and request the change.

Q: Can HALOCAD place a watermark on a drawing?

A: Watermarking is a function of each CAD system and HALOCAD does not modify drawings itself, this is not available at this time. This is under consideration for future development.

Q: Can a default label be assigned?

A: Yes, this would be assigned by the MIP administrator.

Q: How do I set an expiration date on a drawing?

A: Use a label that has an assigned expiration date (example 3 Months) The expiration date must set for a label - for example, Confidential (expires in 3 Months) after which the file cannot be opened by anyone other than the owner.

Q: Can I share a protected drawing with someone outside my organization?

A: Yes. There are two ways: For editing collaboration, install the HALOCAD plugin on the partner's system, register their users with MIP, and obtain HALOCAD licenses for the users. For read only collaboration, install the free Read-Only HALOCAD plugin on the partner's system and register the users in MIP. No license from SECUDE is necessary.

Q: Can HALOCAD restrict print and screen grabbing via the Prnt Scrn key?

A: Labels with print access disabled will provide this feature and labels with copy access disabled will restrict Prnt Scrn, Snipping tool and Microsoft supported tools.

Q: What happens when a user leaves the organization?

A: When a user leaves the organization, all the user's labels can be identified by the Administrator and ownership changed to another active user. The associated models and drawings will continue to have the same privileges as before.

In case, if the user who is moving out is not the owner his user id needs to be removed from the security label.

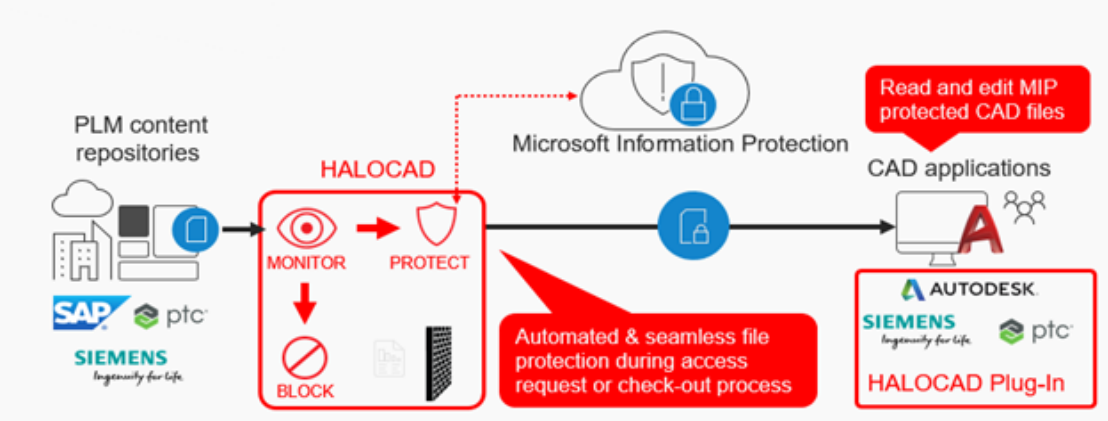
Q: Is it possible to run a proof of concept?

A: Yes. The customers can experience different use cases of HALOCAD with our remote PoC environment on SECUDE Garden4You. SECUDE's GARDEN4YOU is a remote standalone demo environment for performing a PoC with Microsoft Information Protection. The PoC showcases the ability to handle sensitive data from SAP, CAD/PLM using SECUDE's flagship products HALOCORE and HALOCAD respectively.

To know more and schedule a PoC, visit https://secudegarden4you.com

Q: What is the architecture of HALOCAD?

A: Here is the reference architecture of HALOCAD



Q: What is the strength of your encryption that is applied to protected files?

A: We use Microsoft Azure Information Protection SDK for applying the encryption which use the algorithms compliant under FIPS 140-2.

Q: Is it possible to automatically classify CAD models and drawings?

A: HALOCAD uses IP Classification rules in PLM applications to apply labels for CAD models and drawings. For Native CAD applications default label can be enforced for new files based on meta data attributes.

Q: How can users apply label for all parts in a CAD assembly automatically?

A: While selecting and applying a label to a top-level CAD assembly file and if that file contains any of the dependent part/sub-assembly files the same label can be applied to all child components automatically.

INFRASTRUCURE & SECURITY FAQs

Q: What is the prerequisite software for HALOCAD Add-On?

A: Microsoft Information Protection (MIP) or Active Directory Rights Management Service (ADRMS) should be available and active at the customer location.

Q: What tools the partner / supplier need to have pre-installed to access the CAD model/drawings?

A: SECUDE offers a standalone HALOCAD Add-On for CAD applications to read the protected files by authorized users. So, this add-on needs to be installed for the partner / supplier CAD application to open the protected files.

Q: How long does it take to set up HALOCAD?

A: It takes 1 day maximum to install HALOCAD Add-On for CAD applications and 3 days maximum to install the Add-on for PLM applications.

Q: Please describe what plug-ins and server components are needed to support your solution?

A: As already mentioned, HALOCAD is an Add-On implemented on CAD applications as well as on PLM. We also have a couple of server components, one for configuring the classification/action rules and the other which uses MIP SDK to apply the protection.

LICENSE RELATED FAQs

Q: What is the license model for the HALOCAD DRM solution?

A: We have both Perpetual and Subscription licensing model. For PLM users it will be Tier based pricing and for CAD users it will be user-based pricing.

SUPPORT FAQs

Q: What are all the CAD applications currently supported?

A: The following CAD applications are covered.

a) AutoDesk Inventor/AutoCAD
b) PTC Creo
c) Siemens NX, Solid Edge
d) Bentley MicroStation (Planned)
e) Dassault CATIA, SolidWorks (Planned)

Q: What are the PLM applications currently supported?

A: The following PLM applications are covered.

a) PTC Windchill
b) Siemens Teamcenter
c) SAP PLM
d) Bentley ProjectWise (Planned)
e) Dassault Enovia (Planned)

Q: Does HALOCAD support multiple versions of the CAD or PLM applications?

A: HALOCAD has a standard practice of supporting (N-5) versions of the CAD or PLM applications under coverage. N – is the latest released software version in the market.

Q: What features does your solution support/not support for protected files when stored in external or on-line repositories (e.g. Drawing repositories, Box, SharePoint Online, etc.)?

A: HALOCAD provides the protection feature based on Microsoft Information Protection(MIP). So, almost all the features available within MIP protection will be supported. Currently, the user-defined custom labels provided within MIP is not supported.

Q: What file formats does HALOCAD support?

A: The following file formats are supported

1. AutoCAD – dwg, dxf
2. Inventor - ipt, iam, idw, ipn
3. Creo - asm, prt, mfg, drw, frm, lay, s2d
4. NX - prt, jt
5. SolidEdge - par, psm, asm, dft

About SECUDE

SECUDE is an established global security solutions provider offering innovative IT data protection for users of SAP software.

Founded as a joint venture between SAP and Fraunhofer Institute in 1996, SECUDE maintained a close SAP technology partnership and became a reliable resource for security solutions for the SAP market with 'Single Sign-On' for SAP, which was acquired by SAP in 2011. With a focus on making business process for data protection efficient and automated with little or no user interference,SECUDE's goal is to provide ease of use while minimizing cost of rollout and operations.

Leveraging its 20-plus years of experience in SAP security and business process know-how in protecting enterprise IP and data, SECUDE launched HALOCORE® as a holistic approach to protect SAP data exports.

SECUDE's solutions are trusted by many Fortune 500 and DAX listed companies. With branches in Europe, North America and Asia, SECUDE supports customers with the implementation of IT security strategies through a global network.

For more information, visit www.secude.com and follow our social media channels: LinkedIn, Twitter, and YouTube.

SWITZERLAND
SECUDE International AG
Werfestrasse 4 A
6005 Lucerne
Tel: +41 61 366 30 00

INDIA
SECUDE Solutions Pvt. Ltd.
No. T2/6, Dr. VSI Estate
Thiruvanmiyur
Chennai – 600 041
Tel: +91 44 4297 5600

USA
SECUDE IT Security, LLC
5F, 160 East 84th Street
New York, NY 10028
Tel: +1 646 944 6944