SUMMITAI

SummitAI IT Asset Controller

IT Asset Controller

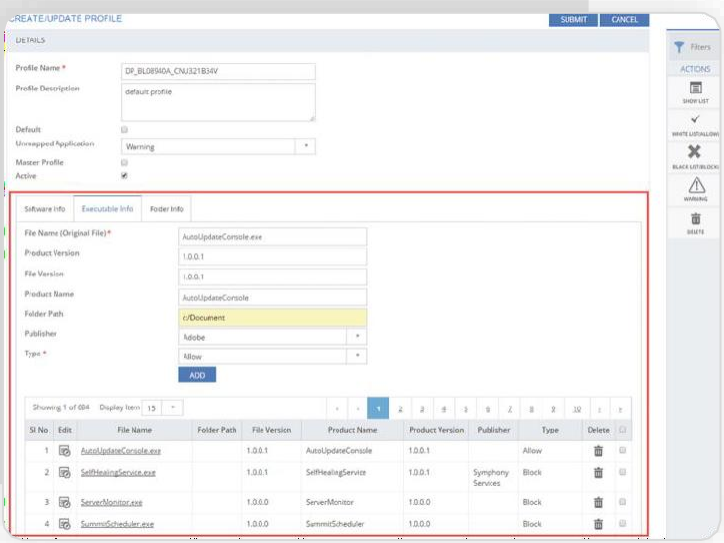
Decision makers of today's IT companies, are more concerned about the security of their networks, protection of their data, and control over their IT assets. SummitAI IT Asset Controller helps organizations enforce IT policies for software installation and execution, thereby, reducing the risk and ensuring compliance. This operational approach- based module is aimed at improving operational efficiency by streamlining software asset management.

Key features

- Application control
- Dynamic built-in local administrator account control
- Endpoint compliance

Application control

The Application Control feature provides an effective way to block the installation and execution of unauthorized software and application on desktops and laptops. These can be installed on a Microsoft Operating System*, even though the end users have Local Administrator access rights. SummitAI's centrally managed innovative solution ensures that only authorized software (whitelisted) can be installed or executed in the device, both 'ON' and 'OFF' network.



SummitAI All rights reserved 2026

Acceptable user policy

Application Control makes it simple to create and enforce acceptable user policies in an organization. With Application Control, software access can be selectively provided or blocked based on the user entitlement, department, job function, or location. After a policy is set, Application Control allows the IT team to view who installed the network, what is installed on it, in real-time. This information can be used to check compliance, evaluate employee needs, and refine acceptable user policies. The Application Control feature extends its coverage to executable files and drivers for greater control over application components.

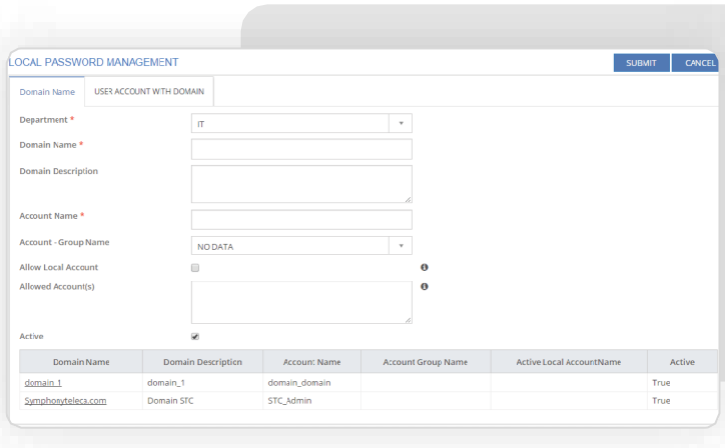
A process can be set where users can request for a new software or application through a Service Request, and the IT team can choose to approve or reject these new requests after they are white-listed. It is also important to educate the desktop/laptop users about 'prohibited' applications with informative pop-up messages that can prompt them to seek approvals via the Service Desk Request. This reduces the risk from unauthorized applications and codes.

More visibility

The IT team can select, report, and govern the usage of applications by using the Application category or Application sub-function.

Dynamic built-in local administrator

Built-in Local Administrator Account passwords are system generated and stored in an encrypted format in the Password Vault available in SummitAI. These passwords are validated regularly and reset to maintain the integrity of the Password Vault.



SummitAI All rights reserved 2026

A built-in Local Administrator Account in laptops or desktops enables users to modify the content/configuration/installation of any software in the device. Local Administrator Account is a crucial account that needs to be critically controlled to avoid any security breaches that may lead to data theft and data loss.

In many organizations, the Local Administrator Account is the most vulnerable area for security breaches. This is because they have a common local admin password across the entire endpoint infrastructure that runs Microsoft Operating Systems*. Controlling the Local Administrator Account then becomes a crucial business activity.

SummitAI Asset Controller provides an effective way to manage the Local Administrator Accounts. It creates a unique password for every Local Administrator Account across the organization. The unique passwords are managed centrally in the Password Vault and the passwords are available on request by select IT Administrators through which the transactions are controlled and tracked.

Endpoint compliance

Today, organizations are challenged by complicated tasks and a variety of governance directives and regulatory mandates require them to implement, monitor, and enforce IT controls to protect endpoint devices. Additionally, organizations face the risk of not always knowing what devices are connected to their networks and not being able to evaluate the compliance status of those devices with their IT policies.

In an attempt to meet the challenges and required compliances, many organizations have made a lot of investments, in endpoint security, such as installing antivirus, personal firewall, and patch management technologies. But to achieve compliance, enhance ROI, and prove the effectiveness of policies, organizations need solutions to help ensure that their endpoint security mechanisms are properly used and their corporate policies are always enforced.

SummitAI offers an extremely effective and unique endpoint compliance solution in the market today. It enables organizations to evaluate, protect, and remediate managed systems, whenever, they connect to corporate assets. It enables administrators to examine system configuration information to ensure that servers, desktops, and laptops stay in compliance with policies and ensure that new endpoints adding on to the network are compliant from the beginning.

SummitAI Endpoint Compliance monitors around 200+ parameters, such as open shares, antivirus, USB, IR bluetooth and password policy enabled or disabled etc., and reports their compliance percentage to the administrators.

SummitAI All rights reserved 2026

Core benefits

- Provides visibility of endpoints connected to the network.
- Ensures that managed endpoints meet minimum protection requirements prior to permitting access to corporate assets.
- Lowers the total cost of ownership by delivering on-demand endpoint protection via the existing web infrastructure.
- Protects endpoints with integrated personal firewall, intrusion detection prevention, and adaptive policies to change the network environment.
- Defends against attacks targeting corporate endpoints.
- Controls the usage of peripheral devices, such as USB drives to help prevent data theft and loss.
- Provides efficient management and reporting capabilities.

About SummitAI

SummitAI, formerly SymphonyAI Enterprise IT, delivers AI-native service and operations for the enterprise. With deep domain knowledge, enterprise context, intelligent ontologies, workflows, and agentic AI, SummitAI understands how organizations operate and turns that intelligence into autonomous action. From service management and asset management to IT operations, security, and enterprise workflows, SummitAI helps organizations resolve more work with less human intervention.

SummitAI is recognized by leading industry analysts, including Gartner, Forrester, and IDC, for its innovation in AI-powered enterprise service and operations.
Learn more at https://summitai.com/

Request a demo or contact us for more information at the bottom:

summitai.com/itsm/get-started
info@summitai.com

SummitAI All rights reserved 2026