

Mbarx Secure IoT

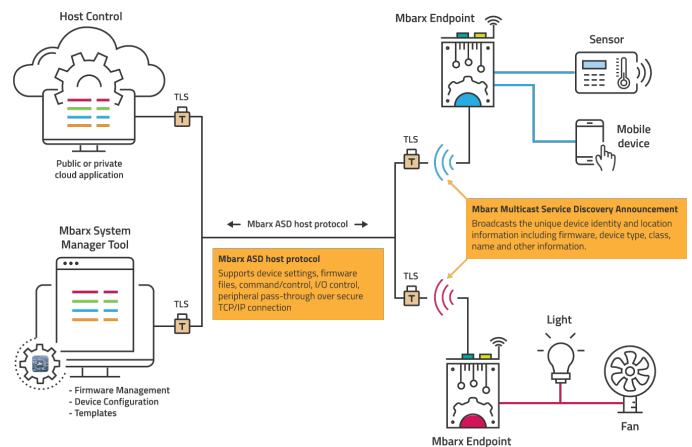
Endpoints, Tools and Gateways

overview

Mbarx simplifies the development of secure, end-to-end IoT systems. It consists of endpoints, tools and gateways that work together to form a chain-of-trust architecture. The Mbarx ecosystem is built around endpoints that range in complexity from simple MCUs to multi-process Linux systems. Mbarx endpoint solutions are intended to provide underpinning security, connectivity, configuration and firmware management services, without defining the core function of the endpoint itself.

Mbarx endpoints provide location and service information to other applications, tools or gateways. This information is used at a system-level to understand the capabilities of the endpoint and securely connect, configure or control it. Mbarx endpoints are built around a security architecture that includes industry standard TLS cryptography with certificate based authentication.

Mbarx tools interact with endpoints. Mbarx System Manager provides administrative workflow at a site-wide level allowing for the configuration and management of many devices concurrently, using simple click-through workflow. When combined with Mbarx gateways, System Manager capability is extended to support remote IoT sites. System Manager is qualified to support hundreds of concurrent firmware upgrades using a conventional PC and is available for Windows® or Mac®.



Endpoint solutions, tools and gateway solutions for secure IoT systems.

Arcturus
empower embedded.

The information supplied by Arcturus Networks Inc. is believed to be accurate and reliable, but in no event shall Arcturus Networks Inc. be liable for any damages whatsoever arising out of the use or inability to use the information or any errors that may appear in this publication. The information is provided as is without any warranties of any kind, either express or implied. Arcturus Networks Inc. reserves the right, without notice, to make changes to the information or to the design and specifications of its hardware and/or software products. Products subject to availability. - Arcturus and the Flying-A logo are trademarks of Arcturus Networks Inc. Linux is a trademark of Linus Torvalds, all other products, services and companies are trademarks of their respective owners.

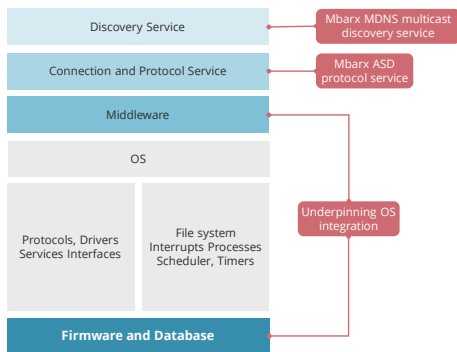
© 2017 Arcturus Networks Inc. v0.5 - subject to change

Arcturus Networks Inc.

701 Evans Ave - Suite 300 Toronto, ON M9C 1A3
Tel: 1.866.733.8647 or 416.621.0125 Fax: 416.621.0190
arcsales@ArcturusNetworks.com
www.ArcturusNetworks.com

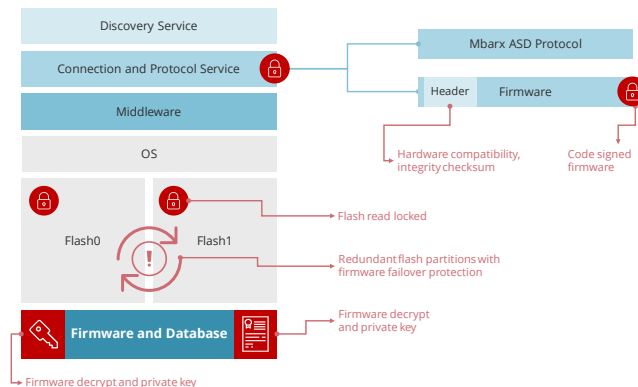
endpoints

The Mbarx endpoint stack consists of two components, a multicast discovery announcement and a point-to-point connection. The discovery announcement advertises basic information using a multicast protocol. The point-to-point connection is established by securely connecting to a TCP/IP socket or local UART connection. This connection provides a simple request/response protocol service that can be used for both configuration, firmware management and operational control.



Security Architecture

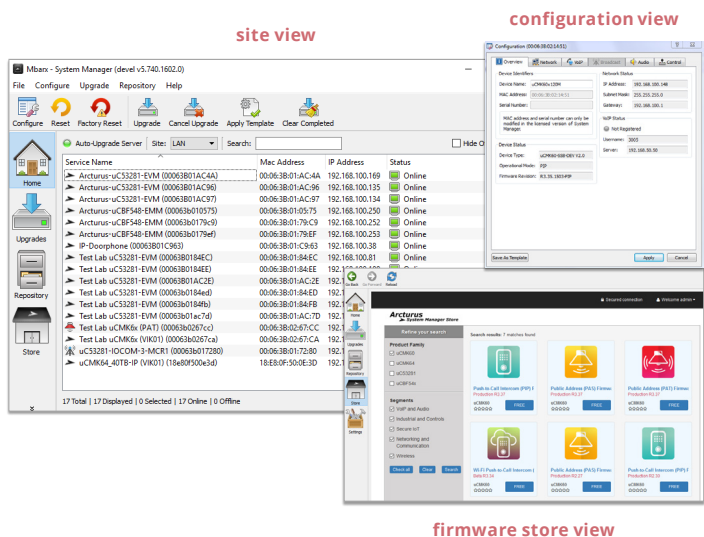
The Mbarx security architecture is built on a foundation of industry standard TLS authentication and encryption, then enhanced to support payload integrity, authenticity and compatibility for system critical functions such as firmware upgrades. This additional protection helps to minimize threat vectors and improve system reliability. Device specific implementations can further enhance this performance with redundant firmware storage, image failover, flash read lockout and tamper detection.



tools

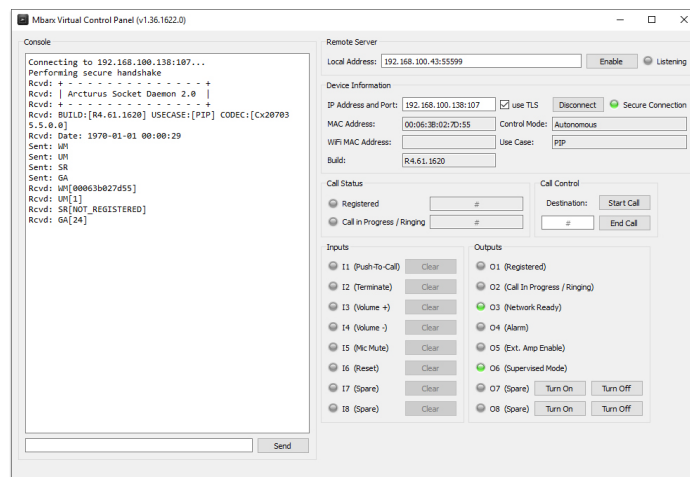
Mbarx System Manager

Mbarx System Manager is a PC tool that supports concurrent configuration and firmware management of many endpoints across a site. System Manager supports bulk templates, firmware, reset, restore and configuration capabilities. It also has an auto-upgrade service that allows endpoints to "call home" to check for updates. System Manager stores firmware in a local repository and connects to a secure cloud store to acquire new firmware from a trusted source. System Manager works with Mbarx gateways, extending capability beyond a local network to manage many IoT sites, from one central location.



Mbarx Virtual Control Panel

The Mbarx Virtual Control Panel is a tool to help developers become familiar with the Mbarx ASD protocol. It contains a console interface and various controls to help with workflow experimentation and debug. The Virtual Control Panel is built using Python and QT and is available as a source package for developers that may want to use it as a starting point. The Virtual Control Panel is available for Windows or Mac.

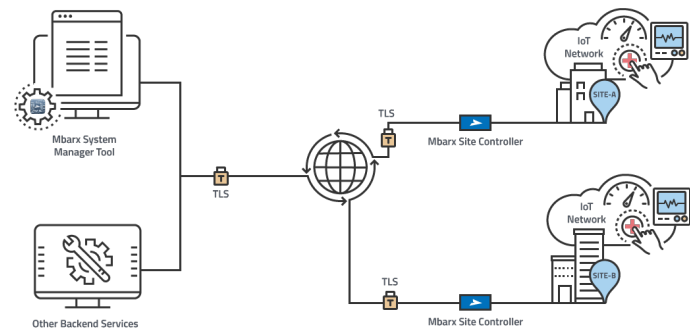


- DEVICE DISCOVERY
- CONFIGURATION MANAGEMENT
- FIRMWARE MANAGEMENT
- REMOTE HOST CONNECTIVITY
- TLS, TRUST-CHAIN ARCHITECTURE

site controller

The Mbarx Site Controller is a gateway solution to meet the secure connectivity and services requirements of IoT sites. The Site Controller resides at the edge or inside a remote IoT network and provides secure access to the site and its endpoints. Site Controllers are compatible with the Mbarx System Manager tool, allowing secure management of many IoT sites, from one central location. Site Controllers can be deployed in networks where multiple subnets or NATs make inbound connectivity difficult and are easily added as deployments change or grow.

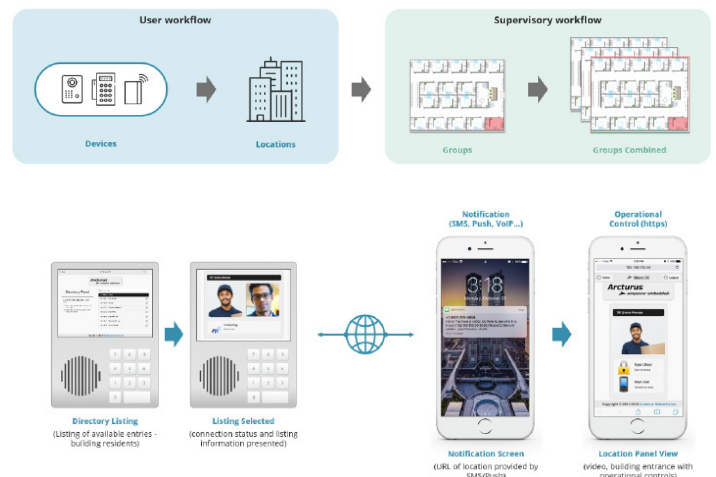
In addition to connectivity, Site Controllers provide various IoT site services, including the ability to host automated firmware deployments. This approach eliminates the need for devices to egress their home network, reducing bandwidth, vulnerability and improving update reliability. The Site Controller firmware upgrade service is qualified to handle 300 concurrent update sessions, using Arcturus IoT Gateway hardware. Site Controllers also provide network services, such as DHCP, NTP and rsyslog or specialized services, such as voice/PBX, network bridging/bonding, failover or 3G/LTE redundancy.



operations controller

The Mbarx Operations Controller gateway solution is intended for developing secure interactive workflow systems. It is suitable for various types of applications where user supervised workflow is required, including security and access control, nurse call, patient care or mass transit management systems. The core is built around a hierarchical grouping and notification system where devices are associated to a location; locations are then grouped hierarchically to form a continuum, such as rooms, floors, buildings etc. The notification system is tied to events that are fed from devices, these events are routed to subscribed users through the Operations Controller framework or externally via push notification, SMS, VoIP, Twitter, or other methods.

The user front-end is a mobile responsive html5 workflow interface. This allows users to jump seamlessly from notification to operational control regardless of where they are in the world or type of fixed or mobile device they are using. The user interface provides the ability to tie in other html objects such as live video, historical information, location, account data etc. The system is multi-user and highly configurable.



availability

Arcturus offers several levels of software, customization, solutions and support.

Endpoints and Tools

IoT development kits are available for endpoints including the uCMK64-IoT module. Tools are provided with the purchase of the development kit. Please refer to the Arcturus website for online ordering information and details.

System Solutions

System Solutions are engineering-level engagements that combine Arcturus hardware, software and expertise to form turn-key project collaborations. System Solutions provide a low-cost barrier to entry to

get projects moving forward and packages are tailored to specific project needs. System Solutions leverage extensive experience developing connected products for healthcare, transportation and building system markets.

Online Gateway Lab

Access to an online lab provides the opportunity to evaluate the capabilities of Mbarx gateways. The lab provides access to standard Mbarx endpoints by securely connecting to the lab's Site Controller. Connectivity to the demo lab is built into System Manager, allowing existing users to remotely evaluate the capabilities of Mbarx gateways in a real-world environment.

- **DEVICE DISCOVERY**
- **CONFIGURATION MANAGEMENT**
- **FIRMWARE MANAGEMENT**
- **REMOTE HOST CONNECTIVITY**
- **TLS, TRUST-CHAIN ARCHITECTURE**