Extreme®
Connect Beyond the Network

Data Sheet

Highlights

Automating Network and IoT Access Without Compromising Security

- Supports any device, any network, any vendor
- Unified Wired and Wireless Access policies
- Ensures consistent and predictable network access for managed and unmanaged devices
- Controls and automates network access for BYOD and IoT devices
- Facilitates regulatory compliance
- Software-only, virtual appliance, extended high availability
- Automated, standards-based
- TACACS+

Identity Engines Product Suite

The Identity Engines Ignition® Server is part of the Identity Engines portfolio—a comprehensive set of software products designed to interwork and simplify network identity and access management, The product suite includes:

- Ignition Server
- Guest and IoT Manager

The Identity Engines product suite integrates with any vendor's networking equipment to provide the central policy decisions needed to enforce role-based network access control while supporting federated identity management across all major corporate directories, e.g., Microsoft Active Directory, LDAP, RSA Authentication Server, Infoblox and more.

Identity Engines Ignition Server

Securing and Automating Today's Network Edge

With up to 50 billion Internet of Things (IoT) devices forecast to come onto the network by 2020, securing and automating network access is imperative. It is essential that IT departments have control and visibility over network access without limiting the flexibility and value these devices deliver for anytime, anywhere productivity and collaboration.

The Identity Engines Ignition® Server is a comprehensive policy engine that uses identity as the basis for managing and monitoring access across your network. It is an easy-to-deploy RADIUS server that connects with your existing identity systems and switch infrastructure. The Ignition® Server provides a central policy decision point that streamlines access management, improves security and satisfies reporting requirements.

The Ignition® Server lets network administrators apply policies that evaluate user account details, switch details, device type and/or any known attribute to determine network access. It supports dynamic session provisioning, allowing each user to be assigned to the appropriate VLAN or VLAN:ISID, based on the attributes of the user and device. It also supports Mobile Device Integration and supports Extreme Network's innovative Fabric technology for automation of the wiring closet edge.

Product Benefits

Improved Security

Policy based access control governs which users can log in and which areas of the network they can access. With Identity Engines, enterprises have granular control of both users AND endpoint devices. The Ignition® Server sets session parameters at login time, allowing VLAN or VLAN:ISID provisioning and the activation of switch-based security features.

Edge Automation

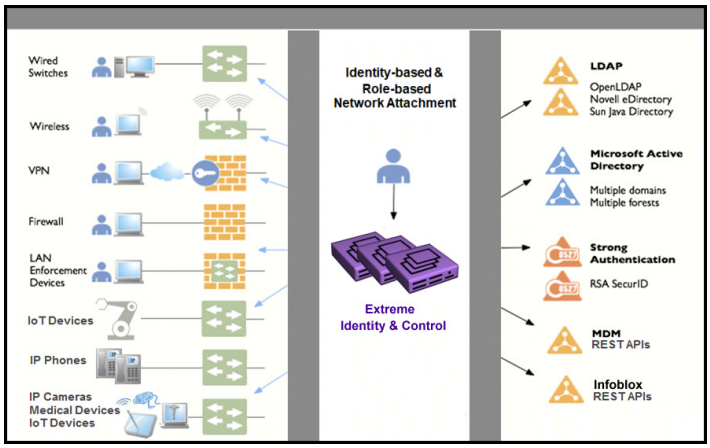
Identity Engines automates network access. The Identity Engines policy server will identify the IoT device that is attempting to attach to the network and based on the access policies for different type of network attached IoTs, Identity Engines will provision the segmented network service required for the device.

Compliance

Identity Engines Ignition® Server provides an accurate view of which users and devices have logged in and offers simple report generation for compliance.

Easy Deployment

The Ignition Server integrates seamlessly with your existing network and directories. Because authentication is performed directly against your enterprise user directories, access policies operate on your latest user account information, reducing latency and helping to ensure consistent security.



Key Features

- **Standards-Based Policy Engine** — Applies access policies consistently and transparently across any network infrastructure wired and wireless.
- **Integration With all Major Directories** — Support for Microsoft Active Directory, Novell eDirectory, SUN Directory Server, Kerberos Services, Oracle Internet Directory, RSA Authentication Server, Token Services, Radius Proxy Services.
- **Identity Routing** — Smart lookup of users lets you determine how the Ignition® Server searches multiple user stores for user credentials, attributes and groups. Smart lookup of endpoint devices e.g. in Infoblox.
- **Dynamic Session Provisioning** — Support for 802.11x assigns each user to an appropriate VLAN, based on the attributes of the user or the context of the login. Change of Authorization (CoA) support.
- **Rich Support for Non-802.1X Devices** — Industry-leading MAC address authentication feature to handle non-802.1X devices such as medical equipment and printers.
- **Fabric Attach Support** — Fabric Attach support for automation of wiring closet edge. Simple and Secure FA Client Authentication, Service Authorization and Creation. Support for FA Proxy Standalone mode in select ERS switches. Inventory for FA clients including most recent location. Recent Fabric Attach enhancements include FA Clients re-servicing, FA Clients Dual Keys and Trusted FA Client.
- **High Availability** — Provides a high availability in a Active-Standby or Active-Active modes.
- **Access Policy Templates** — Support for a variety of use cases make it easy for administrators to copy, paste and apply.
- **Easy Deployment Model** — Integrates seamlessly with your existing network, directories and virtualized infrastructure.