

Extreme Networks Identity Manager



The Situation

As companies routinely handle extremely sensitive and private information for individuals and businesses, they are also faced with the challenge of finding ways to reduce operational risks associated with governing the integrity, security, and privacy of the network and data they manage. Not only does the challenge of identity management move up and down the stack from the hardware layer up to the business application level, but it also moves outside those boundaries to the cloud and virtual computing environments.

The Challenges

Many businesses today are operating in a climate of strict compliance, and are under increasing pressure to achieve enterprise effectiveness. They struggle with managing access rights for enterprise employees, outsourced staff, consultants, and business partners across multiple systems, applications, and platforms used for the business. Organizational changes and rapid workforce growth create a challenge for IT departments in consistently managing wide access rights for users while ensuring access to the right applications at the right time and location.

Companies are increasingly driven by the need to find cost-effective ways to align to business processes, improve productivity, and maintain application availability all while confirming network access requirements. For most enterprises, the ability to control access and monitor the network user, device, and location is currently very limited.

Challenges leading to reduced enterprise effectiveness:

- Handling access control of user accounts and rights on-demand is labor-intensive
- Adapting access rights to changing organizational roles is time-consuming
- Increasing network traffic noise interrupts business productivity and compromises network integrity
- Multiple-point security products, often added as a way to segment the network, require lengthy configuration and manual labor
- Ensuring that regulatory compliance meets audit guidelines is a complex process and requires extensive preparation

Challenges leading to security and compliance deficiency:

- No transparency of enterprise-wide access rights is currently available
- Firewalls' enforcement points create more internal network entry points with more complex policies
- Troubleshooting can take longer and amplify security risks when multiple devices and applications are involved
- Implementing the compliance framework is not automated
- Monitoring wrongfully accumulated access rights is difficult

The Solution

Extreme Networks® Identity Manager feature provides a best-of-breed solution to bring user profiles, device, location, and presence awareness to network managers while enabling enforcement of corporate policies at every network point of entry. Identity Manager provides network-wide viewing and reporting of identities and also helps administrators manage network-wide role-based policies for both users and devices. Applying that intelligence consistently across the network enables seamless mobility and on-demand access to applications to maintain business continuity.



The Benefits

Increase Network Availability	Identity Manager reduces network noise by enabling switches at the network edge to enforce the right policies at the right time, then applying those policies consistently across the network, based on user profiles.
Reduce IT Support Costs for Enterprises	Identity Manager reduces time needed to locate users or devices in the network. EPICenter® network management software and ExtremeXOS® network operating system provide extensive information about identities and their locations, which can reduce IT support and troubleshooting time.
Reduce Compliance and Audit Costs	Identity Manager helps to meet compliance requirements such as HIPAA for healthcare service providers, SOX for enterprises, and those mandated for agencies and organizations in the Federal framework.
Industry Standards-Based Technology	Helps in working with a diverse set of products from server, network equipment, and software vendors.
Leverage Existing Network Infrastructure	To deliver robust network access control existing Summit®, BlackDiamond® 8K, BlackDiamond 10K, and BlackDiamond 12K series switches in the network can be used. This increases ROI and can reduce the total cost of ownership.
Integration with Business Processes and Custom Applications	ExtremeXOS InSite SDK provides the XML APIs to monitor and manage identities, as well as role-based policies from independent third-party applications.
Reduce Training and Other Overhead	ExtremeXOS delivers a consistent CLI framework across the switching products portfolio, and EPICenter provides an intuitive user interface to quickly set up, provision and manage role-based policies.

The Technology

Identity Manager is available in the ExtremeXOS 12.4 operating system or later and EPICenter 7.1 or later, and runs on the existing Extreme Networks enterprise switching portfolio, eliminating the need for a forklift upgrade. The flexible and modular architecture of ExtremeXOS allows for gathering and collecting attributes from different sources on the network (e.g. IT applications and servers), which helps in constructing identities and correlating information from multiple sources.

In future development, role-based access control policies are enforced by configuration through either EPICenter or the ExtremeXOS based switch. An extensible framework based on XML APIs is used for communication between EPICenter and the switches. When user or device identities are discovered, the switch determines if the identity can be placed in one of the configured roles.

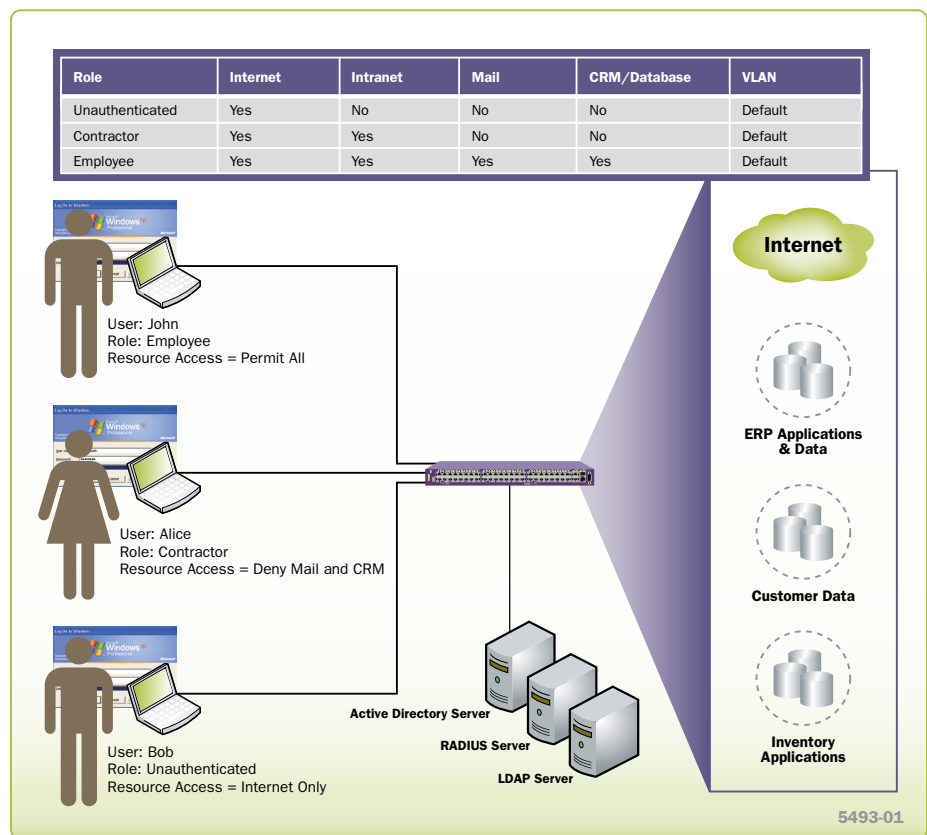


Figure 1: Identity Manager Report



www.extremenetworks.com

Corporate and North America
 Extreme Networks, Inc.
 3585 Monroe Street
 Santa Clara, CA 95051 USA
 Phone +1 408 579 2800

Europe, Middle East, Africa and South America
 Phone +31 30 800 5100

Asia Pacific
 Phone +65 6836 5437

Japan
 Phone +81 3 5842 4011