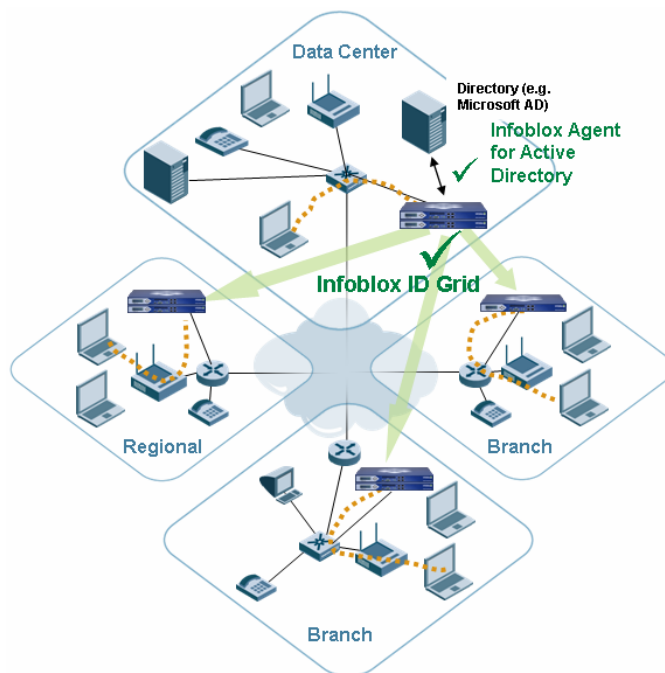


ESSENTIAL NETWORK SERVICES FOR AUTHENTICATION AND 802.1X

The *Infoblox Network Services for Authentication* package provides reliable and highly available authentication services for all major wireless LAN (WLAN) vendors.

802.1X Authentication: New Opportunities, New Challenges

802.1X is the industry standard for authenticating network access, and is the key element for ensuring security in wired and wireless networks and for enabling new security initiatives such as network access control (NAC). 802.1X requires three components: the supplicant, which is software on the client device; the network access device (aka the authenticator), which is typically a wireless access point or a wired switch; and an authentication server, which communicates with the network access device using RADIUS. With 802.1X, the authentication server becomes a key component of the network infrastructure. If the authentication server fails or becomes unreachable, all access to the network may be denied. As such, network authentication services must be deployed with the highest possible reliability, and the overall system design must sustain against the failure of servers or the WAN links among remote network access devices and centralized user directories.



Infoblox Solution: Distributed Appliances with ID Grid Technology

- + Eliminates performance bottleneck
- + Ensures local survivability if a WAN link fails
- + Automatic replication of user credentials to remote appliances via Infoblox ID grid
- + Automatic synchronization of user credentials from Microsoft Active Directory
- + Secure, hardened platform
- + Appliances easily deployed in HA pairs for even higher availability

802.1X Authentication: Infoblox Solution

Infoblox reliably solves all the distribution issues with RADIUS for WLAN services. The solution uses a combination of Infoblox appliances, ID grid technology, and the Infoblox replication agent, software that runs on the Microsoft domain controller and securely replicates user credentials (user names and passwords) from the domain controller to the grid master and stores them in the built-in Infoblox bloxSDB™ database. The credentials are then replicated over a secure VPN to all Infoblox appliances in the grid. When an appliance is deployed in a branch office, it can provide authentication services for 802.1X even during a WAN outage that makes the Infoblox grid master (and the Active Directory server) unreachable. Infoblox NIOS™ software also has built-in hardware based high-availability (HA) technology that provides an extra layer of reliability by enabling appliances to be deployed in redundant pairs. Infoblox solutions work with most major WLAN vendors.

Please contact your local Infoblox sales person or channel partner to get more information.