

Two-Factor Authenticated DHCP Addressing: The MetaInfo SAFE DHCP and Authenex A-Key Solution

IP Network Threats and Challenges

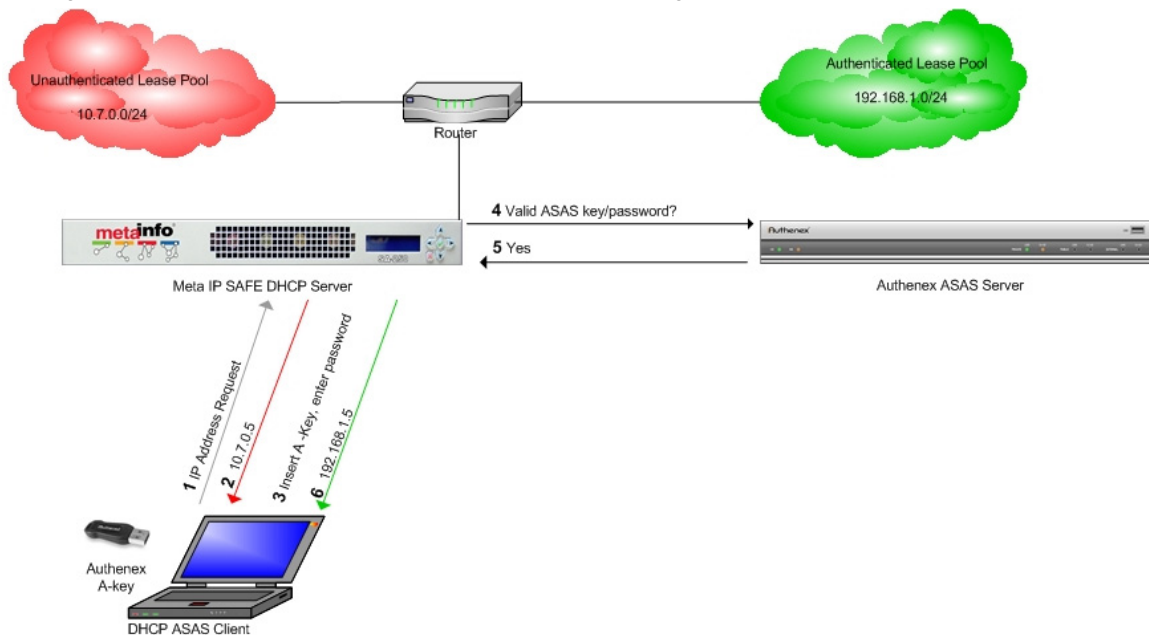
With the increase in reliance of IP networks comes the increase in potential risk and vulnerability surrounding access to that network. One major area of risk is the use of DHCP for dynamic IP addressing. Most IP networks use Dynamic Host Configuration Protocol (DHCP) to automate the allocation of IP addresses and network service information to hosts using the network. This is actually a tremendous vulnerability because DHCP will respond to any request for IP address and host configuration without requiring any authentication.

This leaves the network open and vulnerable to unauthenticated access to IP addresses and network information while enabling the potential release of viruses, worms, or malicious code. In effect, any user can simply connect to the network and receive a DHCP address before any identity verification and authentication occurs.

The MetaInfo & Authenex Solution

Combining the MetaInfo SAFE DHCP IP Key Module and the Authenex A-Key and ASAS server solutions provides a two-factor, strong authentication solution for user authentication and DHCP access providing a secure IP foundation. With this solution the network administrator can configure Meta IP SAFE DHCP to hand out an unauthenticated and restricted IP Address and then require users to authenticate via the A-Key and ASAS server before receiving an authenticated, unrestricted IP address. This delivers an unprecedented ability to strongly validate the user's identity before DHCP hands out a privileged network IP address and information.

In the diagram below, an unknown host requests an IP address. SAFE DHCP responds with an unauthenticated address. The user then inserts the A-key and enters a password. SAFE DHCP requests the ASAS Server validate the A-Key and password. If both are valid, SAFE DHCP issues an authenticated and privileged IP address. Otherwise, the host keeps the non-privileged IP address.



Solution Benefits Summary

- MetaInfo SAFE DHCP never blindly allows IP address allocation to hosts and protects the network from unauthenticated access and attacks by viruses, worms, or malicious code
- The Authenex A-Key and ASAS server enforces strong, two-factor authentication to validate and control user identity and privileges
- The SAFE DHCP IP Key module requires this authentication via the A-Key and ASAS prior to allocating privileged IP addresses and network information

The Meta IP SAFE DHCP IP Key Module combined with the Authenex A-Key and ASAS server clearly protects against the risk of unauthenticated access to key network resources at the IP layer and protects networks from the threat of the accidental release of viruses, worms, and malicious code by unverified network users.

Feature Summary

Meta IP	Authenex A-Key and ASAS
<p>IP Infrastructure Management</p> <ul style="list-style-type: none"> - Centralized Management over distributed DHCP & DNS services - TSIG Authentication Management for services - Secure, encrypted communication with services - Delegated administrative capabilities and permissions - Dynamic data views - IP Network Creation and Management view - Configuration templates - Management replication and scheduled back up of configurations - Advanced logging and intelligent data validation tools - Multiple OS and platform support including hardened appliance versions <p>SAFE DHCP</p> <ul style="list-style-type: none"> - MAC Address Authentication - IP Key Authentication Module - Check Point Authentication Module - Failover - Advanced and Custom Option support - TSIG authentication support - Multiple OS and platform support including hardened appliance versions <p>Meta IP DNS</p> <ul style="list-style-type: none"> - Active Directory integration wizard - Standards-based BIND implementation - Supports Dynamic Updates - Security with ACLs and TSIG Authentication - Advanced configuration capabilities - Multiple OS and platform support including hardened appliance versions 	<p>A-Key</p> <ul style="list-style-type: none"> - Onboard encryption engine using 128-bit Advanced Encryption Standard (AES) to execute challenge/response sequences - Unique Private Shared Secret (PSS) for each A-Key - Multiple Private Shared Secrets allow access to multiple networks with same A-Key - Injection molded for tamper proof safety with small, rugged form factor for convenience and durability - Available with upgrades for OTP and CCID capabilities <p>ASAS</p> <ul style="list-style-type: none"> - No PKI, time synchronization or card-swipe infrastructure needed for deployment and administration - Uses RADIUS and TCP/IP protocols, is VPN and Firewall interoperable, and supports ODBC - Web Management Console allows for remote administration, plus auditing and report capabilities - RADIUS redundancy for ASAS Authentication servers - Database replication and redundancy on Windows platform with Microsoft MSDE and SQL Server