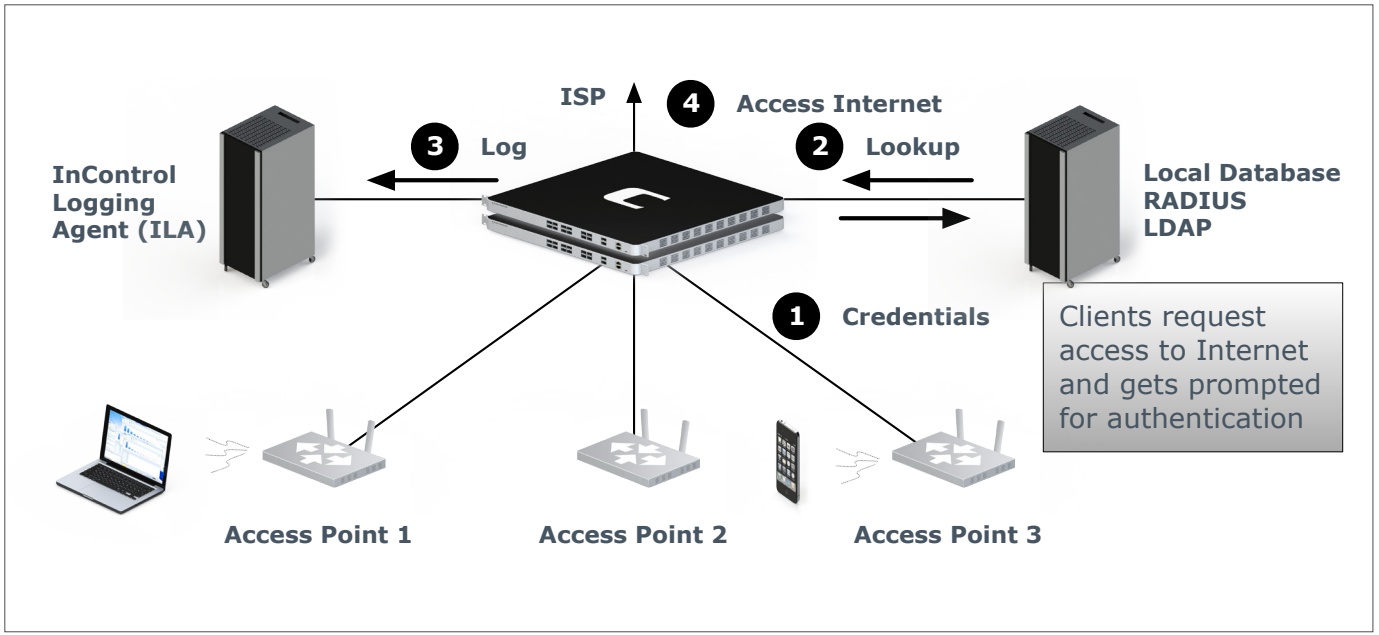
Authentication

Clavister cOS Core productos a base de funciona como solución de autenticación en, por ejemplo, redes WiFi. Cuando un usuario quiere acceder a una página Web, es redirigido a un formulario de autenticación donde deberá introducir su nombre de usuario y contraseña para obtener acceso.



Ejemplo

En este ejemplo, se configura el El Clavister producto para administrar la autentificación usando diferentes orígenes; base de datos local, RADIUS o LDAP. En una red con un amplio número de usuarios, es cómodo tener un o un cluster de servidores centrales los cuales mantienen la información de usuario y es responsable de autentificar y autorizar permisos. Una base de datos de usuarios centralizada y ubicada en uno o más servidores dedicados contiene las credenciales de todos los usuarios, así como los detalles de las conexiones, reduciendo significativamente las tareas administrativas.

1. Un usuario hace una petición para acceder a internet usando un dispositivo. Tal como un Apple iPhone o un portátil. Al usuario se le solicitan las credenciales de autenticación. El formulario que se muestra al usuario puede personalizarse para adaptarse a las necesidades corporativas.
2. Las credenciales introducidas por el usuario se validan en las bases de datos de usuarios configurados.
3. La petición de autentificación se registra.
4. Si las credenciales son correctas el usuario obtiene acceso a internet.

RECURSOS

Para más información de **Authentication**, por favor descargue la guía Clavister cOS Core Administration desde www.clavister.com/my-clavister/downloads/clavister-cos-core

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | www.clavister.com

CID: clavister-sol-solutions-authentication (2012/11)