

Overview of Cisco ScanSafe Cloud Web Security with EasyID

Simple deployment is an important requirement for companies integrating web security into their networks. Cisco® ScanSafe Cloud Web Security offers many deployment options, giving companies the best method to fit their architecture. This white paper provides an overview of EasyID, a new clientless deployment method for enabling the Cisco ScanSafe Cloud Web Security solution.

Seamlessly Embrace the Cloud

EasyID allows customers with Microsoft Active Directory/Lightweight Directory Access Protocol (LDAP) integration to easily deploy Cloud Web Security by enabling user identification and authentication in a browser without installing additional software. Browsing is then allowed with the appropriate policy enforced.

EasyID consists of three elements:

- **User identification:** Users identify themselves in a web browser with their domain user name and password.
- **User authentication:** Identity provisioning introduces the capability to securely access Microsoft Active Directory from Cisco's data center for user authentication. All group associations are available for configuration in the online Cloud Web Security management portal.
- **Browsing persistence:** Once a user is authenticated, a cookie is set so browsing is persistent and every subsequent request does not require a user prompt.

Why EasyID?

- **Simple to deploy:** No hardware or software is required to authenticate and identify users.
- **Operating system-agnostic:** EasyID will work on any device with a web browser that supports cookies, such as iOS or Android tablets and smartphones, but will not provide secure tunneling of traffic or traffic redirection. For seamless laptop support, please refer to the Cisco AnyConnect™ Secure Mobility Solution.
- **LDAP attribute-based filtering:** LDAP attributes can be used, allowing customers to create policies specific to an office location or a selected team of people.

Figure 1. Clientless Authentication with EasyID

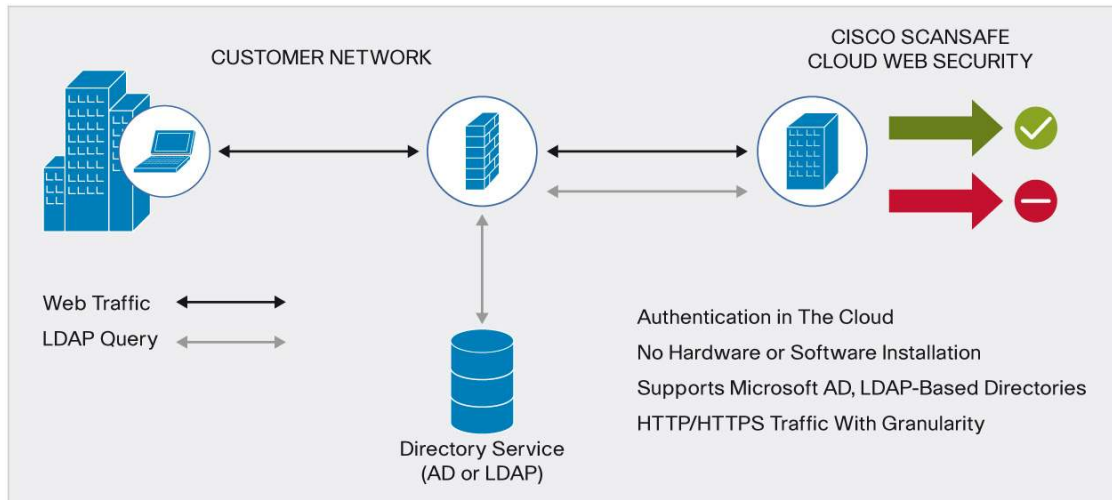
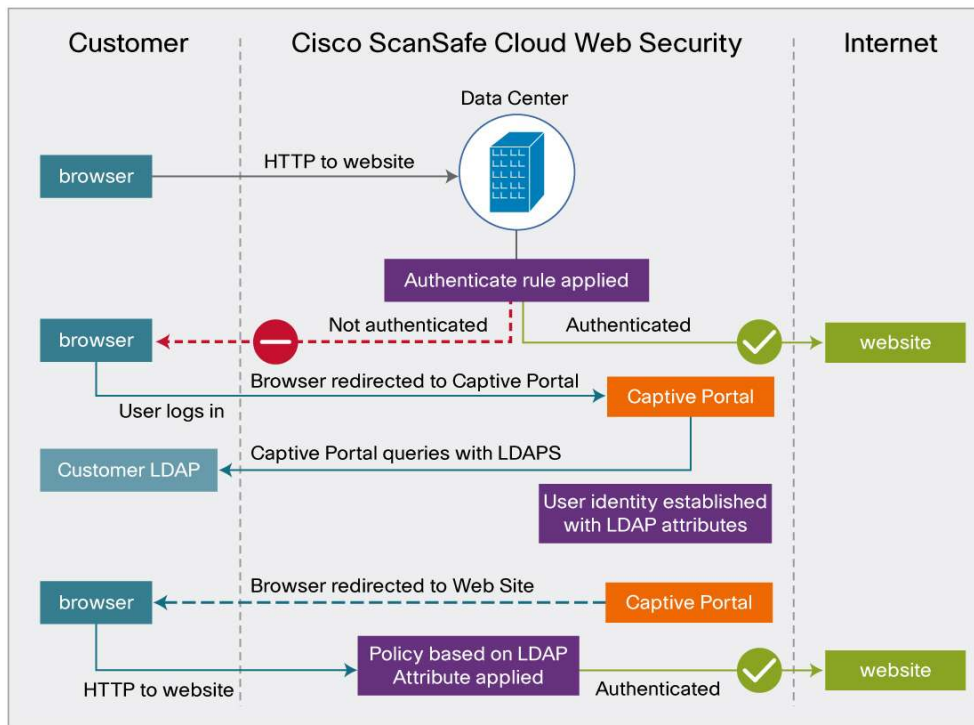


Figure 2. EasyID Transaction Flow



Frequently Asked Questions

- Q.** Where are cookies physically located?
- A.** Every browser type stores cookies in different locations. Typically, cookies are stored in a proprietary database in the user's home directory or in a global directory. Cookies are usually stored with permissions that block casual snooping by others, but are not encrypted.

Q. Are Cisco Cloud Web Security cookies encrypted?

A. Yes.

Q. What types of cookies are supported with EasyID?

A. EasyID supports session cookies in a browser. If cookies have been configured to expire, users will be prompted to authenticate again upon expiration. The cookie verification process weighs the user session time and the configured time within ScanCenter, the intuitive web-based interface for Cisco ScanSafe Cloud Web Security, which integrates all management and reporting capabilities. Session cookies take precedence over persistent cookies to provide a better browsing experience because persistent cookies do not allow administrators to control authentication frequency. For example, persistent cookies set to expire in one week base user authentication on when the last authentication took place, but session cookies authenticate all users at the start of each session.

Q. What information is stored in EasyID cookies?

A. EasyID stores the following data inside a cookie. This data is then compressed, encrypted, and encoded.

- Customer ID number (relevant to Cloud Web Security)
- Unique global ID for the cookie
- Protocol used to verify user and group
- User name
- Group

Q. How secure is Lightweight Directory Access Protocol (LDAP)/Transport Layer Security (TLS) when used to create connections from the cloud?

A. LDAP/TLS is essentially the same authentication and encryption mechanism as Secure HTTP (HTTPS), the standard for secure online transactions. In the recommended network configuration for EasyID, customers only open ports in their firewalls for Cisco Cloud Web Security data centers to access the LDAP server.

Q. What information does EasyID query?

A. EasyID asks LDAP servers two questions:

1. Is this username/password pair valid? (Authentication)
2. What groups is this user a member of? (Identity)

Q. Is traffic a variable for authentication?

A. Yes. The Cisco Cloud Web Security policy engine allows filter actions, such as allow, block or authenticate, to be applied based on user agents. For example, administrators preferring to authenticate or block traffic only in Internet Explorer may now do so.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)