HCL SafeLinx uses standard-based protocols to enable secure access from mobile computing devices outside the firewall to business applications and data on your organization’s internal network. It also gives remote users secure web-based and client-based access to enterprise applications. Supporting an extensive list of standard Internet Protocol (IP) and non-IP wireless bearer networks, server hardware and operating systems, and mobile security protocols, SafeLinx allows remote users to connect to your internal network from a range of desktop, notebook, and handheld mobile devices and operating systems.

HCL SafeLinx supports three types of connectivity:

- **Clientless connections through HTTP access services**
  HTTP access services provide secure, clientless HTTP access for mobile devices that run supported HTTP-based applications. Devices that connect through HTTP access services communicate with internal servers through a secure SSL/TLS tunnel. Applications access is seamless and does not require installation of VPN client software.

- **VPN access through mobile access services**
  Mobile access services provide traditional VPN access to internal network servers and services. Computers and mobile devices that connect through mobile access services must be running the HCL SafeLinx VPN client to access your protected network.

- **Messaging gateway access through messaging services**
  Messaging services enable a web application server to send messages from a wired network to a client on a wireless network.

For both, clientless users and traditional VPN users, HCL SafeLinx provides secure, seamless connectivity with support for authentication, encryption, network optimization, and session persistence.

HCL SafeLinx includes multiple components that you can configure to support connectivity and integrate and manage with other network resources.

To support the needs of your deployment, you add component resources to HCL SafeLinx. Certain components are common to all deployments. For example, every deployment includes an access manager and a Safelinx Server. Other components are optional, and you can add them to the Safelinx Server to support a specific type of network access or security, or to assist you in managing the deployment.

You add components as resources in the Safelinx administration tool and specify their properties. When creating a resource, you assign it to a specific organizational unit (OU).
### What’s new?

Improved functionality of VPN and Reverse Proxy

### Key components

Your HCL SafeLinx deployment includes a range of components. Many components, including the access manager, SafeLinx Server, persistent data storage, and SafeLinx Administrator are common to all deployments. Other components, such as mobile access services, are used only if you support specific types of connections.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Manager</strong></td>
<td>The Access Manager is the server-side process that communicates with the SafeLinx Administrator administrative application to manage configuration information for the SafeLinx Server.</td>
</tr>
<tr>
<td><strong>SafeLinx Server</strong></td>
<td>The SafeLinx Server provides a gateway through which mobile computing devices on a range of external networks connect securely to resources on your organization’s private internal network.</td>
</tr>
<tr>
<td><strong>Persistent Data Storage</strong></td>
<td>The SafeLinx Server needs access to an ODBC-compliant relational database to store configuration information, session data, and accounting and billing information.</td>
</tr>
<tr>
<td><strong>SafeLinx Administrator</strong></td>
<td>The SafeLinx Administrator is the application that you use to configure, monitor, and maintain the resources of one or more SafeLinx Servers.</td>
</tr>
<tr>
<td><strong>Directory Service Servers</strong></td>
<td>A Directory Service Server (DSS) is a resource that designates an external user account database, such as an LDAP server, and provides information on how to connect to it.</td>
</tr>
<tr>
<td><strong>Organizational Units</strong></td>
<td>Organizational units (OUs) are containers that are used to group and isolate resources and, in combination with Access Control Lists (ACL) and ACL profiles, to control administrative access to those resources.</td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
<td>Administrators are users who are authorized to use the SafeLinx Administrator to configure, define maintain, and monitor SafeLinx Server resources.</td>
</tr>
<tr>
<td><strong>HTTP Access Services</strong></td>
<td>HTTP access services enable secure connections between a remote mobile device and HTTP services on the internal network. HTTP access services do not require installation of a virtual private network (VPN) client and are sometimes said to provide clientless access. HTTP access services are secured with Transport Layer Security (TLS) encryption.</td>
</tr>
</tbody>
</table>
### Mobile access services

Mobile access services provide Safelinx Clients with secure, VPN access from external networks so that you can make enterprise applications and data available to your mobile workforce. These services support a wide range of wireless and dial-up networks.

#### Messaging Services

Messaging services enable a web application server to send messages from a wired network to a client on a wireless network.

#### Authentication Profiles

Authentication profiles define how HCL SafeLinx interacts with the authentication server specified in a DSS to authenticate login credentials for HTTP access services or mobile access VPN connections.

#### Certificates

HCL SafeLinx uses X.509 certificates to establish TLS connections between the Safelinx Server and other devices. Certificates can also be used for client authentication.

#### Wireless Password Policies

A wireless password policy defines the rules that govern users’ passwords. When you create a user ID and require a password, you can specify the password policy that applies to the user.

#### Device Resolver

The device resolver works in conjunction with network access servers (NAS) to uniquely identify devices whenever they connect to the network.

#### User Accounts

HCL SafeLinx maintains a user database that contains account information for each user. These user account records can be added to the database in one of two ways, depending on how you manage authentication.

#### Groups

A group is a collection of resources that you designate for combined use.

#### Increased Cognitive Capability

An ACL is a table of access levels for all resource types per organizational unit (OU).

---

### Client roles

The Safelinx Server connects with clients based on which features are installed and configured.

### Features

- Client (VPN) and Clientless (HTTP Access) options
- Push notification proxy for APNs and Google GCM
- Safelinx Client toolkit for Android
- MAC OSX support
- 64Bit client for Linux and MAC OSX
- Cryptography libraries updated to CliC V4
- SafeLinx client tunneling over ATT net client/Cisco ANYNet
- Mobile Iron MDM
- Midpoints MDM
- Local filesystem support
- Multiple LDAP query methods (Round Robin, Failover, Sequential access)
- Currency (LDAP, GSKit, platform, etc.)
- Daily testing, with both in market, and in development HCL Products & Platforms

Benefits

- Robust, mature, security rich and reliable VPN solution
- Broad range of platforms – mobile devices, laptops, desktops
- Clientless HTTP Access
- Easy to implement – No changes to applications or underlying network
- Seamless, non-disruptive roaming when used with VPN Clients
- Scalable and highly available (Server Runs on Windows, Linux and AIX)
- Suitable for use by customers of all sizes and in all industry sectors

Learn more: https://www.hcltechsw.com

Copyright © 2019 HCL Technologies Limited