Socialite Overview

Most of the enterprises today allow access to popular social networks such as LinkedIn, Facebook, Facebook At Work, Twitter, Instagram, and so on for business communication and collaboration. Such communication channels expose enterprises to information leakage and compliance violation risks. Hence, it is essential to control and enable access to social networking sites.

Socialite provides unified access and moderation control to remote administrators to monitor usage of social networking sites and their applications, enabling productive use of the Internet.

Socialite enables Information Technology departments, compliance officers, and supervisors to ensure that their enterprises are aligned within the compliance and corporate policies. Socialite allows remote administrators to store tamper-resistant social networking conversation transcripts to capture the full meaning and intent of the messages.

A web-based interface of the Socialite gives remote administrators the flexibility to control access to social networking sites at a feature or application level. The remote administrator can configure and apply specific security policies to different employee groups and create, view, and audit usage reports.

Using Socialite, you can configure social networking policies for different employee groups to:

- allow or block access to social networking features (specific pages and applications)
- moderate the messages posted by employees
- archive communication content for review and storage

Supported Social Networks

Supported Browsers

Socialite is supported and tested on the following browsers:

<table>
<thead>
<tr>
<th>Supported Browsers</th>
<th>Supported Versions</th>
<th>Supported Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>40.x above</td>
<td>Windows</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>47.0.2526.111 m and above</td>
<td>Windows</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>8, 9, and 11</td>
<td></td>
</tr>
</tbody>
</table>