Design Guidance

This section contains information intended to help plan for SocialMiner installation and deployment.

Advanced UI Options

The SocialMiner user interfaces are designed to be embedded in other web application user interfaces.

If your web site or application doesn't support OpenSocial, then add SocialMiner to a web page by using an iFrame (for example). With this technique you can make a frame sized to show one of the SocialMiner web pages (like the campaign results panel).

Deployment Models

SocialMiner has a single-server, all-in-one, small or large deployment model. You cannot use a load-balancing, split data-center deployment. There is no replication. The solution is not redundant. The best availability solution for SocialMiner is to back it up at a second location using a scheduled backup. In the event of a site loss, you then restore into a new VM.

The server may be deployed inside or outside the corporate firewall in "Intranet" and "Internet" deployment models.

- The Intranet deployment model provides the additional security of corporate network firewalls to reduce the risk of an external party accessing the system. This deployment model is required if SocialMiner must access internal sites, such as an internal forum site. The disadvantage of the Intranet deployment model is that the SocialMiner system cannot be accessed by partners lacking VPN access. It is common for some public relations functions to be externally managed by an agency and offering easy access to the SocialMiner system is very useful. Also, the Intranet deployment model does not allow rendering of SocialMiner OpenSocial Gadgets in public Internet containers such as iGoogle. The Intranet deployment model complicates proxy configuration, however it simplifies directory integration.
- The Internet deployment model puts SocialMiner outside of a corporate firewall. This deployment model relies on the built-in security capabilities of the SocialMiner appliance. This may be acceptable from a security perspective depending on system use and corporate policies. For example, in some applications the SocialMiner system handles 100 percent public postings and there is no disclosure risk associated with a compromised SocialMiner system. The Internet deployment model may complicate directory integration.

SocialMiner can be deployed where some users access the server through a firewall or proxy. For the customer chat interface, the SocialMiner server can be deployed behind a proxy server or firewall to prevent it from being abused or for limiting access by those outside the firewall.

Hardware and Software Specifications

Cisco supports SocialMiner deployment on any hardware provided that SocialMiner is installed with the Cisco provided VMWare OVF.

For the complete list of possible server options, see http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-socialminer.html.

Ports

The following ports are used by SocialMiner. Your firewall configuration may need to be modified to open these ports for SocialMiner.

Port	Used for	Direction	Comments
Port 25	Email notifications	Outward. From SocialMiner to the configured email server.	SocialMiner communicates with the configured email server (that can be in the corporate intranet or on the internet) to send email notifications.

Port	Used for	Direction	Comments
Port 80	HTTP	Bidirectional	Used for unsecure (HTTP) traffic: • From the SocialMiner user interface (browser) or APIs to the SocialMiner server. • From the SocialMiner server to the internet. SocialMiner communicates outward to the internet to fetch social contact information (such as Facebook posts and tweets) over HTTP. • From the internet or corporate website to the SocialMiner server. SocialMiner receives incoming chat and callback requests from the internet or corporate website over HTTP.
Port 443	HTTPS	Bidirectional	The port used for the client browser to access any of the Administration interfaces or User Options interface. It is used for secure (HTTPS) traffic: • From the SocialMiner user interface (browser) or APIs to the SocialMiner server. • From the SocialMiner server to the UCCX server. • From the SocialMiner server to the internet. SocialMiner communicates outward to the internet to fetch social contact information (such as Facebook posts and tweets) over HTTPS. • From the internet or corporate website to the SocialMiner server. SocialMiner receives incoming chat and callback requests from the internet or corporate website over HTTPS.
Port 465 (configurable)	Email notifications SSL/TLS	Outward From SocialMiner to the configured email server.	SocialMiner communicates with the configured email server (that can be in the corporate intranet or on the internet) to send email notifications.
Port 587 (configurable in Unified CCX Administration)	Email (SMTP)	Outward. From SocialMiner to the Exchange Server.	Used by the Email Reply API to send email. The Email Reply API uses SMTP to send a response to a customer email message.
Port 993 (configurable in Unified CCX Administration)	Email (secure IMAP/IMAPS)	Outward. From SocialMiner to the Exchange Server.	Used by email feeds to retrieve email. IMAPS allows email feeds to fetch email from Exchange Servers and allows the Email Reply API to retrieve email and save draft email messages.

Port	Used for	Direction	Comments
Port 1526	Reporting	Inward. From Unified Intelligence Center to the SocialMiner server.	Unified Intelligence Center communicates with SocialMiner to gather reporting information.
Port 3268 (configurable)	Active Directory	Outward. From SocialMiner to the configured Active Directory host	SocialMiner communicates outward to the configured Active Directory host for unsecure Active Directory connections.
Port 3269 (configurable)	Active Directory SSL	Outward. From SocialMiner to the configured Active Directory host	SocialMiner communicates outward to the configured Active Directory host for secure Active Directory connections.
Port 5222 (configurable)	XMPP (IM) notifications using an external XMPP server	Outward. From SocialMiner to the configured XMPP Notifications server.	SocialMiner communicates with the configured XMPP Notifications server (that can be in the corporate intranet or on the internet) to send XMPP (IM) notifications.
Port 5222	Notification Service (XMPP eventing over TCP sockets)	Inward. From Unified CCX to the SocialMiner server.	SocialMiner listens for incoming TCP socket connections to register and receive XMPP events. Unified CCX uses this port to receive social contact events.
Port 7071	Eventing and chat (BOSH)	Bidirectional	The unsecure BOSH connection supports eventing and chat communication between the SocialMiner user interface and the SocialMiner server.
Port 7443 is used for secure BOSH connections to the XMPP eventing server.	Eventing and chat (secure BOSH)	Bidirectional	The secure BOSH connection supports eventing and chat communication between the SocialMiner user interface and the SocialMiner server.
Port 8080	Non-SSL HTTP/1.1 Connector	Bidirectional	The unsecure port used for the client browser to access any of the Administration interfaces or User Options interface.

Port	Used for	Direction	Comments
Port 8443	SSL HTTP/1.1 Connector	Bidirectional	The secure port used for the client browser to access any of the Administration interfaces or User Options interface.
Port 38001 (configurable)	Media routing (in Unified CCE deployments)	Inward. From the Unified CCE MR PG to the SocialMiner server.	The CCE Media Routing Peripheral Gateway (MR PG) communicates over a socket connection to SocialMiner to support the media routing connection.

Provisioning

The following table shows the sizing limits for small and large deployments of a single SocialMiner system.

	Large deployment	Small deployment
Concurrent admin users signed in	5	5
Configured feeds	200	100
Configured campaigns	100	50
Simultaneous chat sessions	400	120
Simultaneous social media users	60	30
Days chat transcript storage	30	30
Tags per social contact	20	20
Callback contacts per minute	40	40
Filters per system	30 (20 max for Bayesian + author combined, 10 max for script filters) **Note:** Each filter type has its own performance implications and performance depends almost entirely on what is in the script filter implementation.	20 (15 max for Bayesian + author combined, 5 max for script filters) With the same note as for the large deployment.
Filters per campaign	10 (5 max for script filters)	10 (5 max for script filters)
Incoming rate of contacts (total per hour)	10,000	10,000

Replies per Twitter account per hour	30 **Note:** This limit is for a default polling interval of 5 minutes. If the polling interval is set lower than 5 minutes, then the limit is reduced depending on usage patterns.	30 **Note:** This limit is for a default polling interval of 5 minutes. If the polling interval is set lower than 5 minutes, then the limit is reduced depending on usage patterns.

Provisioning Considerations for SocialMiner Chat

Retaining Saved Chat Transcripts

A meter on the System Administration panel of the Administration tab shows the current overall SocialMiner disk usage. The meter shows percent usage and hovering over the meter shows the actual number of bytes in use (the same data can be retrieved using the serviceability API).

The Purge Settings section of the panel displays the maximum age a contact can be before it is automatically purged by the system (default is 30 days).

As chat transcripts comprise the majority of disk usage, users can decide how long they wish to retain contacts by using the formula below to calculate the amount of disk space required to retain chat transcripts for one month (assuming the default purge setting of 30 days is kept). Once the average disk space requirement for a month's worth of chat transcripts is calculated, users can determine if they wish to retain contacts for the full 30 days and allocate the appropriate disk space accordingly; or they can choose to purge contacts more frequently.

Note: If SocialMiner starts to run out of disk space, it will purge contacts based on age (the oldest ones being purged first).

Formula to calculate the number of chats per month:

NUMBER_CHATS_MONTH = ACTIVE_CHAT_TIME_MONTH_IN_MIN / DURATION_CHAT_MIN

where:

ACTIVE_CHAT_TIME_MONTH_IN_MIN is the average number of minutes per month that agents spend on chat activities. Assuming that agent activity occurs for 8 hours a day, 7 days a week, 4 weeks a month; the value is 13440 minutes (8*7*4*60).

DURATION_CHAT_MIN is the average duration of a chat in minutes.

Formula to calculate the amount of disk space required per month for chat transcripts:

DISK_SPACE_MONTH = (TR_SIZE + SC_SIZE) * NUMBER_SIMULTANEOUS_CHATS * NUMBER_CHATS_MONTH

where:

TR_SIZE is the average transcript size in Kbytes.

SC_SIZE is the average size of the metadata for a contact in Kbytes (which is normally 3 Kbytes).

NUMBER_SIMULTANEOUS_CHATS is the number of simultaneous chats sessions allowed.

NUMBER_CHATS_MONTH is the value calculated above.

Maximum Network Latency for Chat

The maximum network latency permitted for chat is 250 ms.

Network Bandwidth for Chat

Allocate network bandwidth required for chat based on this formula:

CHAT_NETWORK_BANDWIDTH (in Kbps) = CHAT_SESSIONS_SENDING_MSG_PER_SECOND * AVG_MSG_SIZE

For example, If all 400 sessions are active and 10% of chat sessions are sending messages every second, then 400 * 10/100 = 40 chat sessions are sending message each second.

If the average message size is 1 Kb, then the chat network bandwidth is 40 Kbps.

SocialMiner User Accounts and Security

SocialMiner minimizes the storage of usernames and passwords to reduce the security risk of a compromised system. There is an administration account for the system setup, but all SocialMiner user access is controlled through Active Directory (AD) authentication. There are no SocialMiner user passwords stored on the SocialMiner System.

Users do not need to be manually set up on SocialMiner to access the system. Any user that is authenticated by the Active Directory setup can use the system. If limits on who can use system are required, set up an AD group and configure SocialMiner to only allow access for that group.

AD authenticated users have access to all functions on the system, although panels access could be blocked by blocking certain URLs.

Twitter Accounts and Security

Access to Twitter is achieved using OAuth. When any kind of Twitter feed is created (Twitter search, Twitter stream or Twitter account), the user is prompted to authenticate with Twitter. The authentication token is stored by SocialMiner and grants access to secure information from Twitter (such as direct messages).

Note: The Twitter accounts used for oAuth in all Twitter feed types can be used to Reply/Direct Message to Twitters by all users in SocialMiner without entering the account password (so social media care agents do not need to know the Twitter account password). The capability to use SocialMiner is controlled by Active Directory. The capability to post or perform actions on Twitter is controlled by SocialMiner. SocialMiner also tracks which SocialMiner user (AD account) makes each post. Therefore, it is possible for the enterprise to track which employee posted a tweet when sharing a Twitter account.

VMware Open Virtual Format (OVF)

The SocialMiner system supports one standard OVF Appliance. SocialMiner can only be deployed on servers using VMware ESXi.

See Virtualization for Cisco SocialMiner for more information.

Developer Information

For developer information, including the SocialMiner API documentation and a discussion forum, see Cisco DevNet at https://developer.cisco.com/site/socialminer/overview/. Access to Cisco DevNet requires Cisco account.

You can find training labs at http://docwiki.cisco.com/wiki/SocialMiner_Labs.