System Administration

Most of SocialMiner system administration is performed using the System Administration panel. This section describes the parts of the panel as well as other administrative procedures including backup and restore, managing certificates, and changing the administrator password.

System Administration Panel

Only the SocialMiner Administrator, who is the application user created during install time, can use the administration panel.

The administration panel on the administration tab provides access to system configuration and serviceability tools that must be set up for efficient system use. The top half of the display consists of software version information, server status and system statistic indicators.

Below the indicators are a series of drawers that contain tools for configuring different system aspects (as described below). Use the arrow buttons next to the headings to open the tool drawers.

System Status and Statistics

The top section of the System Administration panel has three types of system status and statistical information:

- Software versions:
  - Application Software Version (the version of the Cisco Unified OS that SocialMiner is running on).
  - Operating System Active Software Version (The current, active SocialMiner version).
  - Operating System Inactive Software Version (the previous, inactive SocialMiner version - if any).
- Server status for:

- Data store
- Indexer
- Runtime
- Eventing and Chat.
- the Hardware profile (a tool tip shows when you hover over the hardware icon to indicate if the system is a small or large deployment).
- the Mail Notifications Server (if configured).
- the external XMPP Notifications Server (used for Instant Messaging notifications, if configured).
- the Connection to CCE Notifications (used for sending notifications to CCE, if configured).

- Three graphical meters show:
  - the incoming rate of all social contacts (per hour) for this server.
  - the number of concurrent signed-in user sessions with SocialMiner, including administrators and other users via web interfaces and other connected applications.
  - the percentage of the disk being used.

  Hover the cursor over these graphs to see information about current statistics and system limits.

The meters help you determine if a server is nearing any limits. If a meter is completely red

- consider asking users to sign out.
- modify your feeds to reduce the number of incoming contacts.
- increase your disk allocation.

Active Directory

SocialMiner uses Active Directory (AD) to manage and administer user access to the system. All users, with the exception of the administration and reporting users, must be configured on a Microsoft Active Directory server to access SocialMiner.

The AD connection permits users configured in AD to access SocialMiner. You can configure the connection to allow access for all users in AD or for only a specific group of users. Multiple, independent groups that require isolated security and permissions should each deploy their own SocialMiner system.

Note If Twitter account feeds are configured on the system, all users are able to see direct messages to the configured Twitter accounts and all users can post from these accounts. SocialMiner tracks which users make which posts. Companies that want to restrict who can make posts need to configure SocialMiner to authenticate with a specific role. If SocialMiner is authenticated with a specific AD role, then only those AD users with that role can use SocialMiner.

To configure AD, open the Active Directory drawer on the System Administration panel and click **Edit**. Enter or modify these fields and then click **Save** when finished.

- **Enabled**: Checkbox. When checked, the AD connection is active. If not checked, then only the administrator can sign into SocialMiner.
- **Host**: Required if Enabled is checked. Provide the host name or IP address of the AD server.
- **Port**: Required if Enabled is checked. Provide the port for AD. The default AD port is 3269. If you are not using SSL, you must change the port to 3268.
- **Use SSL**: Checkbox. Checked by default. Uncheck if not using SSL. When checked, you must exchange security certificates with the AD server before SSL can work (see below).
- **Manager Distinguished Name**: Required if Enabled is checked. Enter the Manager Distinguished Name used to sign in to the AD server. For example, on a default installation of Microsoft AD, the name is :*CN=Administrator, CN=users, DC=MYSERVER, DC=COM*. Replace MYSERVER and COM with your hostname.
- **Manager Password**: Required if Enabled is checked. The password for the AD Manager account.
- **Role Name**: Optional. The AD role or AD group of users who are allowed to access SocialMiner. If this setting is blank or set to "*", then all users in AD are allowed access to SocialMiner.

Exchanging security certificates with AD

To enable SSL for the AD connection, you must first exchange security certificates between the two servers. Enabling SSL is optional, but if you do not enable SSL, then username and password information is not transmitted securely between SocialMiner and the Microsoft AD server.

To exchange security certificates, on the AD server:

1. Verify that the AD server has the Certificate Services service installed.
2. Select **All Programs > Administrative Tools > Certificate Authority**.
3. Expand the domain node and select **Issued Certificates**.
4. Double click the certificate to open it.
5. Open the **Details** tab and click **Copy to file**.
6. An Export wizard opens. In the wizard select **DER encoded binary**.
7. Use the wizard to select a location to save the file.
8. Click **Finish**.

On the SocialMiner Server:

1. Open the Platform Administration drawer on the System Administration panel and select the link to the Unified OS Administration page.
2. Select **Security > Certificate Management**.
3. Click **Upload Certificate**.
4. For the Certificate Name, select **tomcat-trust**.
5. In the Upload File field, select the file to upload by clicking **Browse...** Select the certificate file you saved from the Active Directory server.
6. Click **Upload File**.
7. Restart the Cisco Tomcat service. Using the CLI, run the command **utils service restart Cisco Tomcat**.

Adding users

The Administration user (configured at install) and Reporting user accounts are the only accounts explicitly configured on SocialMiner. The customer care representatives are configured in Microsoft AD.

When these users sign into SocialMiner, successfully authenticate against AD, and begin to take actions on the system; their actions are associated with their AD user ID.

Mail Notifications Server

The mail notifications server settings allow you to configure SMTP information for a mail notifications server. You must configure a mail notifications server if you intend to use the email notification feature.

To configure the mail notifications server, open the Mail Notifications Server drawer on the System Administration panel and click **Edit**. Enter or modify these fields and then click **Save** when finished.

- **Enabled**: Check to enable the mail notifications server connection.
- **Mail Notifications Server Host**: Required if Enabled is checked. The IP address or host name of the mail notifications server. For Gmail, set this to smtp.gmail.com.
- **Mail Notifications Server Port**: Required if Enabled is checked. The port for the mail notifications server. Port 465 is the default for SSL/TLS connections (such as the Gmail SMTP server smtp.gmail.com). For non-SSL/TLS connections, the default port is 25. If you change the port for your mail notifications server from the default, use the new port number for this field.
- **From Email Address**: Required if Enabled is checked. The email address from which emails are sent.
- **Use Authentication**: Check if the user has SMTP authentication to connect to the mail notifications server. When Use Authentication is checked, these two fields become editable.
    - **User Name**: Required if Use Authentication is checked. The user name for signing in.
    - **Password**: Required if Use Authentication is checked. The password for the user name.
- **Use SSL|TLS** : Defaults to checked. Uncheck this if your mail notifications server does not support a secure connection. This must be checked if you are using the Gmail SMTP server (smtp.gmail.com).

Proxy Settings

Note Consult your Network Administrator for the proxy name and port. The same proxy is used across all feeds. If your server is behind a firewall, the SocialMiner Administrator may need to enable the feeds to use a proxy.

To configure the proxy, open the Proxy Settings drawer on the System Administration panel and click **Edit**. Enter or modify these fields and then click **Save** when finished.

- **Enable Proxy**: Checkbox. When checked, feeds are accessed through the proxy server.
- **Hostname**: Required when Enable Proxy is checked. The IP address or hostname of the proxy server.
- **Port**: Required when Enable Proxy is checked. The port for the proxy server.
- **Exclusion Patterns**: You can add and remove host names or IP addresses for servers not requiring a proxy.
    - To add an exclusion, type the exclusion into the text box and click **Add**.
    - To remove an exclusion, select the red **X** to the right of the exclusion.
    - Wildcards are supported. For example“ *.cisco.com” excludes all servers with a cisco.com hostname and “10.86*” excludes all IP addresses starting with 10.86.

Note

- Proxy changes may take up to 30 seconds to take effect.
- The exclusion list is limited to 255 total characters. (There is an additional character per item in the list that acts as a separator.)
- SocialMiner should only need to access a proxy server if it sits behind a corporate network firewall and has to use an http or https proxy server for accessing an outside network. You should not need to give SocialMiner a private NAT address, and doing so is not currently supported.

Public URL Prefix for Chat Invitation

A public prefix can be added to the shortened URL of a chat invitation so that when a chat invitation is sent in a Tweet or a Facebook comment, the link refers to a URL that is accessible from the public network. In order for this to be succesful, use a reverse proxy or the SocialMiner server needs to be hosted in a DMZ. Use this tool to configure that customer-accessible URL.

In order for this to be succesful, use a reverse proxy or the SocialMiner server needs to be hosted in a DMZ. Use this tool to configure that customer-accessible URL.

Click the **Edit** button to enter a valid URL starting with http:// and click **Save**.

The defined prefix appears in the chat invitation link sent to the customer.

Note

Public URL Prefix for Chat Invitation does not apply to SocialMiner integration with CCX for multisession web chat feature.

CCE Configuration for Multichannel Routing

Use this drawer to configure the media routing peripheral gateway (MR PG) server and a port.

To configure the MR PG server, open the CCE Configuration for Multichannel Routing drawer and click **Edit**. Enter or modify these fields and then click **Save** when finished.

- **Enabled**: Checkbox. Check to enable the media routing server connection.
  - If not enabled, the MR PG configuration will be ignored and no connections will be accepted.
  - If enabled but no hosts are set, then any connection will be accepted.
- **Port**: The MR PG server port that SocialMiner listens to. The port is set to 38001 by default. The valid range is 10000 - 65535.

XMPP Notifications Server

XMPP notifications server settings allow you to configure an XMPP notifications server so SocialMiner can use instant messaging (IM) notifications. You must configure an XMPP notifications server if you intend to use the IM notification feature.

To configure the XMPP notifications server, open the XMPP Notifications Server drawer and click **Edit**. Enter or modify these fields and then click **Save** when finished.

- **Enabled**: Checkbox. Check to enable the XMPP notifications server connection.
- **XMPP Service Lookup**: Check to enable XMPP Service Lookup. When enabled, the User Name's domain is used to connect to the correct XMPP Notifications Server.
- **XMPP Notifications Server Host**: The IP address or Hostname of the XMPP Notifications Server. This does not apply if XMPP Service Lookup is checked.
- **XMPP Notifications Server Port**: The port for the XMPP Notifications Server. This is set for port 5222 by default. This does not apply if XMPP Service Lookup is checked.
- **User Name**: The user name (in full JID format, such as user@domain.name), which is used to sign in to the XMPP Notifications Server.
- **Password**: The password for the above User Name. NOTE: If you change your XMPP password for any reason, change it here.

Purge Settings

Database purges are required to remove old data from the data store so that the disk does not fill up. Data store purges occur on a continuous basis (every hour) based on the age of the contacts and disk usage.

The purge runs automatically 5 minutes after the runtime is started and then runs every 60 minutes. Each time the purge runs, the first 30,000 contacts that are older than the number of days specified in the 'Purge Social Contacts older than (days)' setting are deleted. If no contacts meet the criteria, no contacts are purged. If more than 30,000 contacts meet the criteria, only the first 30,000 are deleted. The next 30,000 are deleted at the next purge 60 minutes later.

Important! Purge settings take effect as soon as you click **Save**; therefore, if the 'Emergency purge when disk usage exceeds (%)' criterion is met, the purge starts immediately.

To configure purge settings, open the Purge Settings drawer and click **Edit**. Enter or modify these fields and then click **Save** when finished.

- Data store purge settings:
  - **Purge Social Contacts older than (days)**: Social contacts older than the specified number of days are purged. The default value is 30. You can change the default value to retain social contacts for a lesser or greater number of days. The value must be an integer (no decimals) between 1 and 550.
  - **Emergency purge when disk usage exceeds (%)**: Begin an emergency purge if disk usage exceeds this value. Valid values are 40–90. When an emergency purge executes, social contacts older than the number of days specified above are removed. If disk usage is still above the setting for this field, the purge continues removing social contacts (one day at a time) until the disk usage is below the threshold for emergency purge.
- Reporting purge settings:
  - **Purge start time (HH:mm 24 hour format)**: The time, in 24 hour format (00:00 to 23:59), that the purge starts based on the local server time. By default this is set to 01:00 (1am) local server time.
  - **Purge Social Contacts older than (days)**:Reporting records for social contacts older than this number of days are purged when the purge starts. Values must be integers (no decimals) between 1 and 550.

Reporting Configuration

The reporting configuration allows you to set or change the Informix password for the reporting user. You cannot change the reporting user name; it is always "reportinguser". This username does not display until you edit and enter a password.

The reporting user is used by Cisco Unified Intelligence Center (CUIC) and third-party applications to access the reporting database. Details on the tables in the reporting database are available in the *SocialMiner Developer Guide*.

To set or change the password for the reporting user, open the Reporting Configuration drawer and enter a new password in the password field, and then click **Save**. Password is the only field you can edit.

You will also see reporting server and database information in this drawer. This information is required for third-party connection to the database. The details include:

- **Reporting Host**: the hostname to use when connecting to the reporting database.
- **Reporting Port**: the port for the reporting database server.
- **Reporting Server**: the Informix server name for the reporting database. When configuring CUIC, this is the "Instance".
- **Reporting Database**: the Informix database name for reporting.
- **Database Type**: the type of database (Informix).

When configuring CUIC, you must select UTF-8 as the character set.

RTMT Download

Use the RTMT (Real-Time Monitoring Tool) to troubleshoot issues in SocialMiner by downloading and analyzing the service logs. You can download RTMT logs for the following services:

- SocialMiner Datastore Service
- SocialMiner Indexer Service
- SocialMiner Migration
- SocialMiner ORM Service
- SocialMiner Public REST API
- SocialMiner REST API
- SocialMiner Runtime Service
- SocialMiner XMPP Server Service

For more information about using RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* available here:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

RTMT Download Links

Links are provided in the RTMT Download drawer to download the Unified Real Time Monitoring Tool (RTMT).

For details on installing and configuring RTMT, see Cisco Unified Real-Time Monitoring Tool Administration Guide.

Audit Logs

SocialMiner 11.6 supports audit logging to keep track of changes made to configuration entities (e.g. Feeds/Campaigns, etc). It also identifies the id used to autheticate the request. The log file can be viewed via RTMT tool by selecting the SocialMiner rest API option. The file titled **ccp-audit.log** is located at : */var/log/active/mmca/logs/ccp-audit.log*

An audit log entry will contain the following fields:

Field	Description
DATE TIME (e.g : 2016-10-27 18:44:55.405)	The date and time when the audit log entry was created .
METHOD	The HTTP request type of the request (e.g PUT/POST/DELETE/GET)
USER ID	The id used for authntication.
URL	The URL context used while requesting.
PAYLOAD	The request data sent as part of the request.
OPERATION	Textual description of the change e.g < CREATE | MODIFY | DELETE>

Log files can accomodate upto 100 MB of data, post which new files will get created. Old files earlier than 6 months will be archived. The audit log files can be viewed via RTMT tool by selecting the SocialMiner rest API option.

To retrieve the audit log file later, use the following CLI command from the admin prompt: **file get activelog mmca/logs/ccpapi/ccp-audit.log**

Platform Administration

The Platform Administration drawer provides links to the following interfaces of Cisco Unified OS:

- *Cisco Unified Operating System Administration*—Use tools on this interface to upgrade software and to import certificates.
- *Cisco Unified Serviceability*—Only shows OS logs, SocialMiner logs are accessed from the System Logs drawer.

Note Though configuration for SNMP alerts is available, SocialMiner does not support SNMP alerts.

- *Disaster Recovery System*—Use tools on this interface to perform back up and restore actions.

SocialMiner uses the same platform administration tools as Unified Communications Manager. Online help is available with the tools.

System Logs

The System Logs drawer provides a link to perform a system health snapshot.

Important! Do not select the System Health Snapshot link unless directed to by Cisco TAC. Accessing this link forces the system to stream all system parameters into a large XML file for download. System performance is impacted while the snapshot is occurring.

Language Pack

Download and install the language pack only if you want to see the SocialMiner interface in a language other than English.

The language pack for SocialMiner is delivered as a single COP file, the same way that SocialMiner delivers COP files for patches. The file is available to download from Cisco.com at the following link:

http://software.cisco.com/download/type.html?mdfid=283613136&i=rm

The file contains a single installer for all language variants. The filename is of the format:

ccp-language-pack_18-11.6.1.10000-x.cop.sgn

where *11.6.1* is the release identifier.

Follow the instructions in Cisco SocialMiner User Guide to install the COP file for the language you want on your SocialMiner interface.

Certificates

Certificates are used to create secure communication between clients and servers. Users can purchase certificates from a certificate authority (CA-signed certificates) or they can use self-signed certificates.

Obtaining a CA-Signed Certificate

Each time you sign-in, the browser validates the certificate presented by the server. If the certificate is not signed by a trusted root Certificate Authority (CA), the browser will typically not allow the connection until the user explicitly allows it. In order to avoid this, you must obtain a root certificate signed by a CA and install it onto SocialMiner.

To Obtain the Certificates

1. Log in to the Cisco Unified OS Administration page using the URL: *https://<FQDN>/cmplatform*.
2. Select **Security** > **Certificate Management** > **Generate CSR**.
3. After the successful generation, click **Download CSR**.
4. Use the CSR to obtain the signed application certificate and the CA root certificate from the CA.

To Upload the Certificates

1. When you receive the certificates, open the Cisco Unified OS Administration page using the URL: *https://<FQDN>/cmplatform*.
2. Select **Security** > **Certificate Management** > **Upload Certificate**.
3. Select the certificate name from the Certificate Name list.

4. Upload the root certificate.
   a. In the Upload dialog box, select **tomcat trust** from the drop-down.
   b. Browse to the file and click **Open**.
   c. Click **Upload File**.
5. Upload the application certificate.
   a. In the Upload dialog box, select **tomcat** from the drop-down.
   b. Enter the name of the CA root in the Root Certificate text box.
   c. Browse to the file and click **Open**.
   d. Click **Upload File**.

For more information about CA-signed certificates, see the Security topics in the Unified OS Administration online help.

After You Upload the Certificates

For the uploaded certificates to take effect, do the following:

1. Restart the XMPP Service. (SSH to SocialMiner and enter the command *utils service restart CCP XMPP Server* as an administrator in the Commad Line Interface).
2. Restart the Cisco Tomcat service. (SSH to SocialMiner and enter the command *utils service restart Cisco Tomcat* as an administrator in the Command Line Interface).

Self-Signed Certificates

Self-signed certificates (as the name implies) are signed by the same entity whose identity they certify, as opposed to being signed by a certificate authority. Self-signed certificates are not considered to be as secure as CA certificates, but they are used by default in many applications (including SocialMiner).

Browsers handle self-signed certificates in different ways. The sections below describe how to handle self-signed certificates on the browsers supported for SocialMiner.

Internet Explorer and Self-Signed Certificates

When using an IE browser on a Windows machine, make sure your DNS server is properly configured and you can resolve the fully qualified SocialMiner hostname to the SocialMiner address. Use a signed certificate from a trusted certificate authority (like Verisign).

If you use a self-signed certificate (which is what is installed with SocialMiner), follow these steps to avoid getting certificate warnings each time you sign in.

- In your Start menu, right click on IE and select "Run as Administrator".
- Enter the URL for your SocialMiner server in the address bar.
- When prompted by the security warning, click on **Continue to this website (not recommended)**.

- Your address bar turns red and you see a certificate error next to the address bar. Select the certificate error.
- Select **View certificates** at the bottom of the popup. This opens a certificate dialog.
- On the General tab, select **Install Certificate...**.
- The certificate export wizard launches. Click **Next**.
- When prompted for where to store the certificates, select **Place all certificates in the following store**, then click **Browse** and select **Trusted Root Certification Authorities**.
- Click **Ok**, then click **Next** and **Finish** to complete the certificate import wizard.
- Click **Yes** when prompted about importing the certificate.
- Close and restart your browser to access SocialMiner.

Firefox and Self-Signed Certificates

Due to changes in the Firefox security model, there are additional self-signed certificates that must be accepted to use the SocialMiner web application on Firefox.

When accessing a SocialMiner server using a newly installed Firefox browser (any version), Firefox attempts to connect to the main port that SocialMiner uses first (port 443). If it cannot connect, it prompts the user to accept the self-signed certificate.

Note If pop ups are blocked, you are given instructions on how to manually launch the certificate page. Also, if the certificate window is closed before the certificate is accepted, the page will automatically re-launch.

- If prompted, click **I Understand the Risks**, then click **Add Exception**.
- Click **Confirm Security Exception**.

Next, Firefox attempts to connect to port 7443 (the secure XMPP port). With Firefox, a second self-signed certificate must now be accepted to use this port. SocialMiner displays a "Checking Connectivity..." screen during this process

If the"Checking Connectivity..." screen persists after a few seconds, click **Continue** to proceed to the Firefox certificate acceptance screen (as above).

Click **I Understand the Risks**, then **Add Exception**, and **Confirm Security Exception** again.

Users need only go through this process the first time they use a new Firefox browser and self-signed certificates. After the certificates are in place, users may not see the "Checking Connectivity..." screen (or it will appear briefly and proceed to the SocialMiner sign on screen).

Google Chrome and Self-Signed Certificates

When accessing a SocialMiner server using Google Chrome Browser, it attempts to establish a Private secure connection using port 7443.

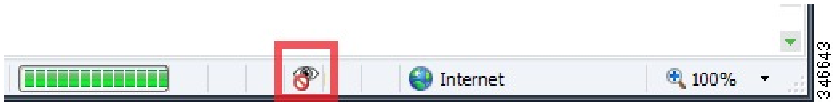
- After keying in the Server IP address in Chrome, the browser displays a connection warning stating **"Your Connection is not private**." To proceed with a secure connection, click **Advanced**.

- Click **Proceed to <Server IP Address>.** Next, Chrome attempts to connect to port 7443 (the secure XMPP port).
- The browser displays **"Checking connectivity**." Click **Continue** to proceed. This opens another Chrome tab, where you are prompted with another connection warning.
- Click **Advanced.**
- Upon clicking **"Proceed to <Server IP Address>",** the SocialMiner log on page is displayed.

Note Users need to go through this process only the first time they use a new Chrome browser and self-signed certificates.

Avoid Sign in Overlays if the Reply Template Container Loads in an IFRAME in IE

When a SocialMiner reply template container loads in an IFRAME in Internet Explorer, a SocialMiner sign in overlay may appear even though SocialMiner successfully authenticated. If the page inside the IFRAME does not have a privacy policy, cookies are blocked (which is indicated by the red barred circle over the 'eye' icon in status bar).



To permit cookies for SocialMiner

1. Select the eye icon. The Internet Explorer privacy settings dialog box appears and displays the blocked cookie from SocialMiner.
2. Select the cookie and choose **Always allow cookie from this website**.

For more information on how to permit cookies, see the Microsoft Windows help site.

Command Line Interface

To access the command line interface (CLI) for SocialMiner:

- SSH to the address for your SocialMiner server.
- Sign in with your administrator credentials.
- Type a "?" at the **admin:** prompt to see the list of commands. Most CLI commands do not apply to or have not been certified for SocialMiner.

For more information, See Cisco Systems CLI documentation.

Control Hack Lock Feature

Hack Lock feature is a security feature which prevents brute-force password attacks by locking out an administrator account from being accessed for a period of 30 minutes.

The administrator can control Hack Lock feature in SocialMiner and can enable or disable it based on requirements.

utils ccp hack-lock enable

This command enables the Hack Lock feature.

Syntax

utils ccp hack-lock enable

Example

```
admin: utils ccp hack-lock enable

Hack Lock feature is successfully enabled.
```

utils ccp hack-lock disable

This command disables the Hack Lock feature.

Warning By default, the Hack Lock feature is enabled. Disabling the Hock Lock feature makes your system vulnerable to brute-force password attacks.

Syntax

utils ccp hack-lock disable

Example

```
admin:utils ccp hack-lock disable

WARNING! Disabling Hack Lock feature can make your system vulnerable to Brute-Force
 password attacks
(attempts to guess passwords using trial-and-error).

Do you want to proceed? (yes/no): yes

Hack Lock feature is successfully disabled.
```

utils ccp hack-lock reset-counters

This command resets the Hack Lock counters in SocialMiner.

Syntax

utils ccp hack-lock reset-counters

Example

```
admin: utils ccp hack-lock reset-counters

Hack Lock counters reset successfully.
```

utils ccp hack-lock status

This command allows you to view the current status of Hack Lock settings in SocialMiner.

Syntax

utils ccp hack-lock status

Example

```
admin: utils ccp hack-lock status

Hack Lock feature is currently ENABLED.
```

Control Logging and Trace Levels

SocialMiner provides commands to show and set logging and trace levels for the following components:

- Runtime
- Webapp

The following logging levels are available to be set:

- Basic
- Detailed

show ccptrace runtime server

This command displays the log level and trace masks for the given subsystem.

Syntax

show ccptrace runtimeserver [subsystem]

Note

The subsystem refers to the one whose log level and trace mask is being displayed here. It is a mandatory parameter and is case-sensitive in nature.

The list of valid subsystems are:

- Infrastructure
- OAMP_BO
- FILTER
- FEED
- CAMPAIGN
- DATASTORE
- REPORTING

Example

```
admin: show ccptrace runtimeserver FEED
The log level is Basic.
```

show ccptrace webapp

This command displays the log level and trace masks for the given subsystem..

Syntax

show ccptrace webapp [subsystem]

Note

The subsystem refers to the one whose log level and trace mask is being displayed here. It is a mandatory parameter and is case-sensitive in nature.

The list of valid subsystems are:

- Infrastructure
- OAMP_BO
- MSGPROXY

Example

```
admin: show ccptrace webapp MSQPROXY
The log level is Basic.
```

set ccptrace

This command sets the log level and trace masks for the given subsystem.

The logging level can be set to either basic or detailed.

There only two valid trace masks which are defined for all the subsystems except Infrastructure, where a lot more granularity is possible:

- TRACE_NONE
- TRACE_ALL

The trace masks for Infrastructure are:

- TRACE_HANDLED_EXCEPTION
- TRACE_JMX
- TRACE_JMS
- TRACE_HEARTBEAT
- TRACE_PARAM
- TRACE_CALL
- TRACE_MESSAGE
- TRACE_NOTIFICATION
- TRACE_GENERAL_CFG
- TRACE_OOOQUEUE
- TRACE_METHOD
- TRACE_LOW_LEVEL

Syntax

set ccptrace subsystem|infrastructure basic|detailed runtimeserver|webapp [subsystem][trace_masks xx]

Note The subsystem refers to the one whose log level and trace mask is being displayed here. It is a mandatory parameter and is case-sensitive in nature.

Atleast one of the trace masks are required which are also case-sensitive in nature.

Example

```
admin: set ccptrace subsystem basic runtimeserver FEED TRACE_NONE
Log level and trace masks updated successfully.
```

TLS Configuration Commands

TLS Configuration Commands are used to configure TLS versions for the inbound and outbound traffic in SocialMiner.

The following commands are available to configure TLS.

set tls server min-version

This command sets user entered minimum TLS version for all inbound secure connections to the one specified in the version.

Note A system restart is required for the changes to take effect.

Syntax

set tls server min-version [version number]

Example

```
admin:set tls server min-version 1.2
```

set tls client min-version

This command sets user entered minimum TLS version for all outbound secure connections to the one specified.

Note A system restart is required for the changes to take effect.

Syntax

set tls client min-version [version number]

Example

```
admin:set tls client min-version 1.2
```

show tls client min-version

This command displays the minimum supported TLS version for the outgoing connection.

Syntax

show tls client min-version

Example

```
admin:show tls client min-version
The client tls min-version is set to 1.2
```

show tls server min-version

This command displays the minimum supported TLS version for the incoming connection.

Syntax

show tls server min-version

Example

```
admin:show tls server min-version
The server tls min-version is set to 1.2
```

Supported Commands and User Interface Options

The following tables describe the VOS Command Line Interface (CLI) commands and the Cisco Unified OS Administration and Disaster Recovery System user interface options that SocialMiner supports.

Only the commands and options explicitly mentioned as supported below are supported by SocialMiner. Any commands or options not listed are not supported.

However, in select instances, users may be instructed to use commands that are not normally supported (such as in a field notice).

Note Although this guide provides instructions for accessing SocialMiner CLI admin commands, most of the CLI commands do not apply to or have not been certified for use on SocialMiner.

Command Line Interface

This table specifies the VOS CLI commands that are supported, and indicates certain ones that are not.

Command	Supported?
delete	No
file	No
help	Yes
quit	Yes
run	No
set date	Yes
set timezone	Yes
set ccptrace runtimeserver	Yes
set ccptrace webapp	Yes
All other **set** commands	No
show	Yes
unset	No
utils network ping	Yes

Command	Supported?
utils reset_application_ui_administrator_name	Yes
utils reset_application_ui_administrator_password	Yes
utils service list	Yes
utils service restart	Yes
utils service start	Yes
utils service stop	Yes
utils system restart	Yes
utils system shutdown	Yes
utils system switch-version	Yes
utils system upgrade	Yes
utils ccp hack-lock enable	Yes
utils ccp hack-lock disable	Yes
utils ccp hack-lock reset	Yes
utils ccp hack-lock status	Yes
All other **utils** commands	No

Cisco Unified OS Administration User Interface

This table specifies the Administration user interface commands and options that are supported, and indicates certain ones that are not.

Command	Supported?
Show	Yes
Settings > NTP Servers	Yes
Settings > Time	Yes
All other **Settings** menu options	No
Security > Certificate Management	Yes
All other **Security** menu options	No
Software Upgrades > Install/Upgrade	Yes
All other **Software Upgrades** menu options	No
Services > Ping	Yes
All other **Services** menu options	No
Help	Yes

Disaster Recovery System User Interface

This table specifies the disaster recovery system commands and options that are supported, and indicates certain ones that are not.

Command	Supported?
Backup > Backup Device	Yes
Backup > Manual Backup	Yes
Backup > History	Yes
Backup > Current Status	Yes
Backup > Scheduler	Yes
Restore	Yes
Help	Yes

System Backup and Restore

SocialMiner supports the Unified OS *Disaster Recovery System* (DRS) to perform backup and restore of the system. You access the Disaster Recovery System by going to the Administration panel, expanding the section on **Platform Administration**, and then selecting the link for **Disaster Recovery System**.

SocialMiner uses the same platform administration tools as Unified Communications Manager. Online help is available with the tools.

You can manually back up your system using DRS or schedule DRS to perform automatic backups.

Details on using DRS are available in the DRS online help and in this guide: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html.

Quick Manual Backup Instructions

These instructions provide the information required to create a manual backup. You must still schedule backups to run automatically.

Note The system is not usable and new contacts are not collected during a backup. Schedule your backups accordingly.

The online help for the Disaster Recovery System provides complete details on all features of DRS. However, using DRS with SocialMiner is greatly simplified because SocialMiner supports only a single node and only uses network backups.

Define Backup Device

Procedure

Step 1 Access the Disaster Recovery System. On the Administration panel, open the **Platform Administration** drawer and then select the **Cisco Disaster Recovery System** link.

Step 2 Sign in using the platform credentials you supplied when you installed SocialMiner.

Step 3 Select **Backup** > **Backup Device**.

Step 4 On the Backup Device List page, select **Add New**.

Step 5 Provide a **Device Name** for the backup device. SocialMiner only supports backing up to a network directory. Provide the network directory details for a server that supports SFTP.

Step 6 Provide the number of backups to store on the network directory. The default is two, so only the two latest backups are preserved.

Step 7 Click **Save**. The system verifies the information you entered and saves the backup device.

You do not need to repeat these steps the next time you back up the system unless you want to back up to a different device or change the backup device settings.

Backup the System to the Backup Device

Procedure

Step 1 Access the Disaster Recovery System. On the Administration panel, open the **Platform Administration** drawer and then select the **Cisco Disaster Recovery System** link.

Step 2 Sign in using the platform credentials you supplied when you installed SocialMiner.

Step 3 Select **Backup** > **Manual Backup**.

Step 4 Select the backup device you created earlier from the drop-down menu in **Select Backup Device**.

Step 5 In **Selected Features**, check **SOCIALMINER**.

Step 6 Click **Start Backup**.

Step 7 A warning appears indicating that you may need to use the security password if you try to restore later. Click **OK**. The backup begins.

Step 8 The backup page refreshes periodically providing the status of the backup. The page also displays the name of the backup tar file that is being saved to the remote system.

Step 9 After the backup completes, wait a few minutes before using SocialMiner (so the SocialMiner system can restart subsystems that were shutdown during the backup).

Restore From a Backup File

Procedure

Step 1 Access the Disaster Recovery System. On the Administration panel, open the **Platform Administration** drawer and then select the **Cisco Disaster Recovery System** link.

Step 2 Sign in using the platform credentials you supplied when you installed SocialMiner.

Step 3 Select **Restore** > **Restore Wizard**.

Step 4 Select the backup device from the drop-down menu and select **Next**.

Step 5 Select the backup file you want to use from the *Tar file list* drop-down menu and select **Next**.

Step 6 In **Selected Features** check **SocialMinerCCP** and click **Next**.

Step 7 On the warning on the page, select **File Integrity Check**, then select the Server to be restored (typically the host name of the backed up system). Click **Restore**.

Step 8 The restoration status page refreshes periodically. When the restoration is complete, restart SocialMiner.

Change the SocialMiner Administrator Username and Password Using the CLI

Use the following procedure to change the SocialMiner Administrator username and password using the CLI.

Procedure

Step 1 Sign in using your current administrator credentials.

Step 2 To change the administrator username, run the command **utils reset_application_ui_administrator_name** and follow the prompts.

Step 3 To change the administrator password, run the command **utils reset_application_ui_administrator_password** and follow the prompts.

Reset the Unified OS Platform Administrator Password

Use the following procedure to reset the Unified OS Platform Administrator password.

Note During this procedure, you must remove any CD or DVD from the disk drive (if any) and then insert a valid CD or DVD into the disk drive to prove that you have physical access to the system.

Before you begin

You must have a keyboard and monitor connected to the server. You cannot reset a password when the system is connected through a secure shell session.

Procedure

Step 1 Sign in to the system using the following credentials:

a) Username: **pwrecovery**
b) Password: **pwreset**

The **Welcome to platform password reset** window appears.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that the disk drive is empty.

Step 5 Insert a valid CD or DVD into the disk drive. You must use a data CD, not a music CD. The system tests to ensure that you inserted the disk.

Step 6 After the system verifies that you inserted the disk, you are prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.
The password must contain at least six characters. The system checks the new password for strength. If the password does not pass the strength check, you are prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password is reset, and you are prompted to press any key to exit the password reset utility.