SocialMiner Installation

SocialMiner is installed as an appliance using the Cisco Unified Communications Operating System (Unified OS). The operating system and the SocialMiner application are installed together using a similar installation process as other Unified OS products such as Cisco Unified Communications Manager and Cisco Unified Intelligence Center.

SocialMiner operates on a VMware Virtual Machine (VM) on hardware that is running a VMware Host Server. SocialMiner currently supports installation of only a single node (as opposed to a duplexed or redundant system).

Note Cisco does not support changing the hostname or IP address on any server once they have been set.

By default, access to SocialMiner administration user interface is restricted. Administrator can provide access by whitelisting client's IP addresses and revoke by removing the client's IP from the whitelist.

For more information, see Control SocialMiner Application Access, on page 2. This section provides the CLI commands to manage the whitelisted IP addresses.

Install SocialMiner

Perform the following steps to install SocialMiner:

Procedure

Step 1 Create a virtual machine using a VMware Open Virtual Format template.

Step 2 Use the respective version specific OVA template for the fresh installation of SocialMiner.

Note Ensure that Cisco SocialMiner OVA template is deployed for a successful install. The install stops if no Cisco SocialMiner OVA template is found in the deployment.

a) Go to https://software.cisco.com/download/type.html?mdfid=283613136&flowid=73189 and download this template.

The Cisco SocialMiner version specific Virtual Server Template (OVA) defines a virtual machine configuration that is supported in the respective SocialMiner release version. This OVA contains all supported virtual machine configurations of this release.

Step 3 When deploying the template, select either a large or a small deployment from the drop-down list.

Step 4 Mount the SocialMiner DVD or ISO file to the virtual machine and set the virtual machine to boot from the SocialMiner DVD. The installation wizard opens. Use Tab to navigate between elements and then press the space bar or the Enter key to select the element and proceed.

Step 5 Perform the media check when prompted.

Step 6 Follow the instructions on the screen and select **Yes** or **Continue**.

Step 7 Use the arrow keys to highlight the correct time zone and then use Tab to navigate to the **OK** button. Press **Enter** to proceed.

Step 8 Provide the network information for SocialMiner. You must provide valid hostname with matching IP address. The system confirms that the hostname matches the IP address later in the installation process.

Step 9 Select **Yes** to provide DNS Client Settings for SocialMiner. Provide DNS servers and the domain. Select **OK**.

Step 10 Provide an Administrator ID and password. This credentials is for platform (Unified OS) administration.

Step 11 Provide information about your organization. This information generates the security (SSL) certificates for this server.

Step 12 You must provide at least one NTP Server. Enter the NTP host address and select **OK**.

Step 13 Provide a security password.

Step 14 Provide a username and password for the SocialMiner administrator. You can import additional SocialMiner users from Active Directory after the SocialMiner installation is complete.

Step 15 The confirmation window opens. You can select **Back** to change settings or **OK** to complete the installation. Installation can take up to two hours. The server may reboot to complete the installation steps. If you install from an ISO file and see the virtual machine message to "Disconnect anyway (and override the lock)?", select **Yes**.

A sign-in prompt appears on the server console.

Step 16 After the installation is complete, perform the one-time setup tasks listed in Additional Configuration Options, on page 4.

Control SocialMiner Application Access

By default, access to SocialMiner administration user interface is restricted. Administrator can provide access by whitelisting client's IP addresses and revoke by removing the client's IP from the whitelist. For any modification to whitelist to take effect, Cisco Tomcat must be restarted.

Note IP address range and subnet masks are not supported.

utils whitelist admin_ui list

This command displays all the whitelisted IP addresses. This list is used to authorize the source of the incoming requests.

Syntax

utils whitelist admin_ui list

Example

```
admin: utils whitelist admin_ui list

Admin UI whitelist is:
10.232.20.31
10.232.20.32
10.232.20.33
10.232.20.34
```

utils whitelist admin_ui add

This command adds the provided IP address to the whitelisted addresses.

Syntax

utils whitelist admin_ui add

Example

```
admin:utils whitelist admin_ui add 10.232.20.33

Successfully added IP: 10.232.20.33 to the whitelist

Restart Cisco Tomcat for the changes to take effect
```

utils whitelist admin_ui delete

This command deletes the provided IP address from the whitelist.

Syntax

utils whitelist admin_ui delete

Example

```
admin:utils whitelist admin_ui delete 10.232.20.34

Successfully deleted IP: 10.232.20.34 from the whitelist
```

```
Restart Cisco Tomcat for the changes to take effect
```

Additional Configuration Options

Procedure

Step 1 If your system is installed behind a firewall, set up an HTTP proxy so that feeds can access sites on the Internet.

Step 2 Configure Active Directory so that additional users can sign in.

Step 3 If you want to use Cisco Unified Intelligence Center, set up the reporting user so that the reporting tool can access the reporting database.