System Accounts on the Cisco Vision Dynamic Signage Director Servers

This module describes the default system accounts implemented by Cisco Vision Dynamic Signage Director for access and control of certain server functions. Aside from the admin account, these system accounts are generally separate from the user accounts that secure access to the Cisco Vision Dynamic Signage Director feature configuration and operation.

In addition, only a few of these accounts are intended for general modification after installation of the server. Other system accounts are reserved for special services or technical support and should not be modified unless you are instructed to do so, or you otherwise understand the impact to your server installation.

For information about user accounts and Role-Based Access Control (RBAC) in Cisco Vision Dynamic Signage Director, see User Management in Cisco Vision Dynamic Signage Director, page 79.

Contents

Information About System Accounts

All of the system accounts are automatically implemented upon installation of the Dynamic Signage Director software.

This section provides an overview of the default system accounts in Cisco Vision Dynamic Signage Director:

Common System Accounts

Table 1 on page 72 describes the common system accounts for Cisco Vision Dynamic Signage Director that are intended for you to modify after deployment of your server, and on which server platform they are supported. These common system accounts are automatically implemented upon installation of the Dynamic Signage Director software.

Table 1 Description of Common System Accounts

Account	Purpose	Server Platform
Admin	**Cisco Vision Dynamic Signage Director** Account that provides access to the administrator RBAC functions in the Cisco Vision Dynamic Signage Director user interface(UI).[1] It is automatically implemented upon installation of the Dynamic Signage Director software. The username is: **admin** The default password is: **C-V1$i0n** Using the Text Utility Interface (TUI) to change the admin account password allows an installer to recover access to the Cisco Vision Dynamic Signage Director UI. The password for the admin user account can also be changed in the Cisco Vision Dynamic Signage Director **Configuration > User** or by setting the option to force a password change upon initial login with the admin account.	Cisco Vision Dynamic Signage Director
Installer	Account that provides access to the TUI using a directly-connected console or SSH client. The username is: **installer** The default password is: **cisco!123**.[2]	Cisco Vision Dynamic Signage Director
TAC (Technical Assistance Center) Access	Account that provides access by Cisco TAC personnel to help troubleshoot an issue. A menu item under System Accounts in the TUI: **a) Enable/Disable TAC user.** For more information, see Enable/Disable TAC User, page 75.	Cisco Vision Dynamic Signage Director

1. For more information on the administrator role in Cisco Vision Dynamic Signage Director, see User Management in Cisco Vision Dynamic Signage Director, page 79.
2. For more information about the TUI, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 109.

Note: We *strongly recommend* you change the password as one of the post-installation tasks. Be advised: there is no way to recover it if lost.

2.

New Password Policies

For tighter security, users must set stronger passwords. When setting a new password, use the following rules:

- Must have at least 1 lower case character (a-z).
- Must have at least 1 upper case character (A-Z).

- Must have at least 1 numerical character (0-9).
- Must have at least 1 special character. Special characters are ! @ # $ %
- Must be 8-127 characters.
- Must not contain any of the following characters: space tab newline linefeed backslash (\).
- Must not contain a character sequence from a predefined list maintained in a dictionary.
- Must not have 3 sequential characters (for example: abc5#pqr is not allowed)
- Must not have a character repeat 4 times (for example: aaaa#2020! is not allowed)
- Dictionary words not allowed: words that look like “cisco,” “password,” and “admin.”

Note: There are two **Generate Password** buttons: when user first logs in and in the **User** screen to create a user (**Configuration > User**). The button provides a random password that meets the password rules. Use the “eye” icon to see the new password.

- After logging in to Cisco Vision Director, the UI displays a brief message about when you last logged in, successfully or not.
- If you try to login with failed passwords 5 times in 1 minute or less, your account is temporarily locked for 30 minutes. Upon next successful login, the message shows that the account was locked due to too many failed attempts.
- In **User** interface, the “admin” role cannot be deleted.

Notes:

1. Every user can change their own password by entering the current one as a challenge.
2. The Administrator can change anyone’s password without any challenge.
3. Except password, other fields of the user’s, like email, can be changed without any challenge.
4. Now password entry has an expiry notification.

5. Whenever a user is created or a password gets changed, the change date is logged.

Passwords after Upgrading

When upgrading an existing installation, existing passwords are kept.

Passwords after Fresh Install

Role: Admin

During fresh install, the default admin user is prompted to change the password on the first login. Starting with Release 6.1, the new password must adhere to the password policies or the password is rejected.

DMP Admin Password

The default password for fresh install is C-V1$i0n. If you do not choose a valid password, the error message indicates which rule is non-compliant.

Other System Accounts

Table 2 describes some other default system accounts that are reserved for use in Cisco Vision troubleshooting or other specialized access.

Table 2 Description of Reserved System Accounts

Account	Purpose	Server Platform
admgr	Reserved for use by special agreement with Cisco Systems to support the Media Planner Import API.[1]	Cisco Vision Dynamic Signage Director
MySQL	Reserved for internal use only to access the MySQL database account.	Cisco Vision Dynamic Signage Director
TAC user[2]	Reserved for troubleshooting with remote shell access. This account should remain disabled and only activated when instructed by Cisco Technical Support for troubleshooting.	Cisco Vision Dynamic Signage Director

1. For more information about the Media Planner Import API and other API support in Cisco Vision Dynamic Signage Director, see the *Cisco Vision Dynamic Signage Director Operations Guide, Release 6.4*.
2. For more information about the TAC user account, see Enable/Disable TAC User, page 75.

Enable/Disable Browser Inspector

A new security enhancement includes disabling the DMPs browser inspector, by default. If you choose to add the registry setting to enable the browser inspector, it stays enabled until and unless you remove the registry data completely and reboot the DMPs. Disabling the browser inspector protects against network access to the DMPs.

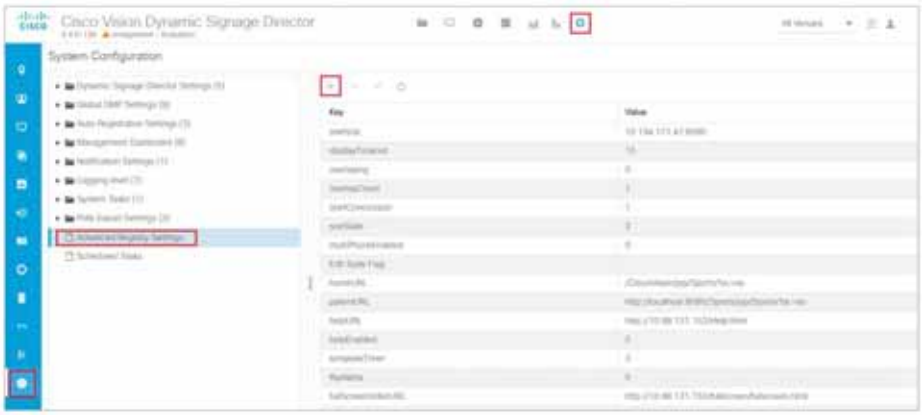
To enable browser inspector, contact Cisco Technical Assistance Center (TAC).

1. Click **Configuration > System Configuration > Advanced Registry Settings**.
2. In **Registry Data**, click **Add** (Figure 1 on page 75).
3. In the Create Configuration Setting dialog box, type **device.SvDmp.browser.inspector.addresses**.

   For example, the address of 192.168.1.1.10.1.1.1 will enable the browser inspector function on the DMPs with the IP address of 192.168.1.1.10.1.1.1.

   Note: For multiple addresses, separate the IP addresses with a comma.

Figure 1 Adding Browser Inspector Address to Registry Data



4. Reboot the DMP for changes to take effect.

To disable browser inspector capabilities:

1. Remove IP address from list.
2. Empty list or remove key to disable completely.
3. Reboot the DMP for changes to take effect.

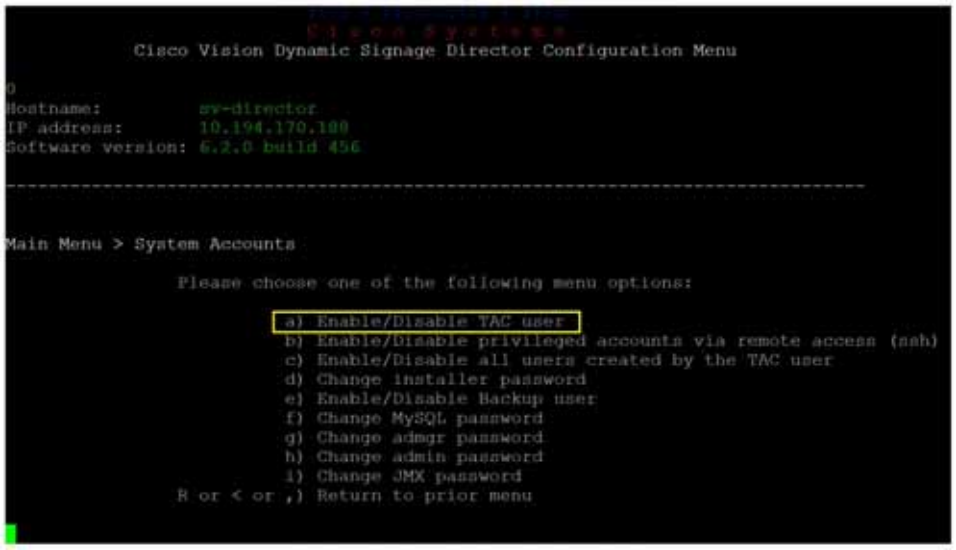
Enable/Disable TAC User

New to Release 6.2, you can create a Cisco TAC User account so Cisco can aid you in troubleshooting an issue. If you create a TAC case and grant access to Cisco TAC personnel, it is best practice to remove Cisco TAC access when the case is resolved.

To enable a TAC user:

1. Login to the Director TUI using the valid user ID and password.
2. Type **b** for **System Accounts**.
3. Type **a** for **Enable/Disable TAC user** (Figure 2 on page 76).
4. Type **a** or **b**.

Figure 2 Enable/Disable TAC User



If you are using this option for the first time, you must set a password. Type it twice.

Figure 3 First Time TAC Account Password Change

Note: Choose a strong password with more than 8 characters, upper and lower case letters, numbers, and special characters. Read the instructions. Keep the credentials you choose because Cisco TAC will not have access to them and cannot recover them for you.

Note: To change the “installer” password (choice **d** above) requires the user to provide the current “installer” password.

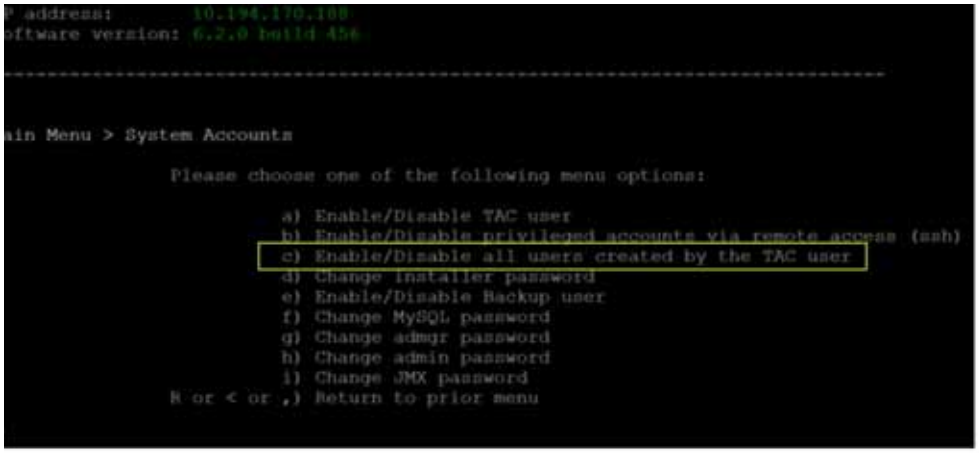
Enable/Disable all Users Created by TAC User

For added security, disable any and all accounts TAC may have enabled to help you solve an issue.

To disable any accounts created by a TAC user:

1. Login to the Director TUI using the valid user ID and password.
2. Type **b** for **System Accounts**.
3. Type **c** for **Enable/Disable all users created by the TAC user** (Figure 4 on page 77).
4. Type **a** or **b**.

Figure 4 Disable All Users Created by the TAC User



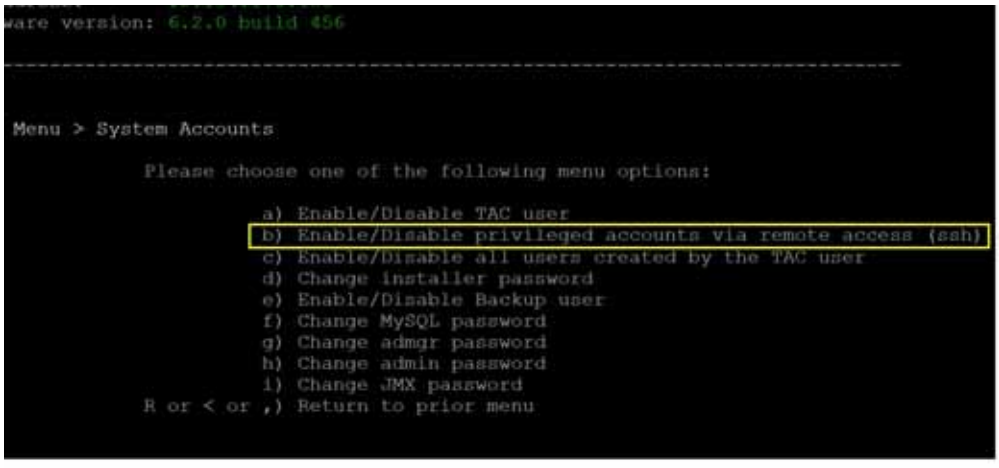
Enable/Disable Privileged Accounts Via Remote Access (SSH)

For added security, disable any remote access to your account.

To disable any remote access via SSH:

1. Login to the Director TUI using the valid user ID and password.
2. Type **b** for **System Accounts**.
3. Type **b** for **Enable/Disable privileged accounts via remote access ssh** (Figure 4 on page 77).
4. Type **a** or **b**.

Figure 5 Disable Privileged Accounts Via Remote Access



How to Change System Account Passwords

You can change system account passwords from the defaults in Cisco Vision Dynamic Signage Director using the TUI.

Note: To navigate through the TUI menus you must type the character that corresponds to the menu area where you want to go (a, b, c, and so on) and press Enter. To return to other menus, you must back out of the hierarchy of menus using one of the indicated keys to return you to prior menus.

To change system account passwords:

1. On the Cisco Vision Dynamic Signage Director, log into the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Dynamic Signage Director network to run a secure login to the primary Cisco Vision Dynamic Signage Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, go to **System Accounts**.
3. Select the system account whose password you want to change.
4. At the prompt, type the new password.
5. When prompted to confirm, retype the password.
6. Press any key to return to the System Accounts menu.
7. Return to the Main Menu and exit the TUI.