CHAPTER 9

DMP Access and Security Settings

Revised: June 1, 2011

Concepts

Understand DMP User Accounts and Passwords

You use the *Web Account* when you log in to DMPDM itself.

In contrast, the *Service Account* is a user account with FTP and SFTP login privileges. It is available only on DMPs whose FTP service is enabled.

Note **Unless or until you change these passwords individually, they are both identical to the master password that you configured in the "Log in" section on page 7-1.** You can change them when they should differ. However, they will become identical again in the future if you edit the master password.

Related Topics

- Understand Whether to Change DMP Passwords Centrally, page 9-2
- Manage and Edit Passwords, page 9-5

Understand Whether to Change DMP Passwords Centrally

Scenario	Best Practice
You have very few DMPs and will manage each of them in isolation.	Use DMPDM to change their DMP Web Account and DMP Service Account passwords one at a time, manually.
You have many DMPs and will manage them centrally.	Use the fully licensed Cisco Digital Signs software on your Digital Media Manager appliance to change both passwords globally for all of the DMPs that you have added to a DMP group. **Note** Before you can manage any DMP centrally, you must configure it to support centralized management.

Related Topics

- Manage and Edit Passwords, page 9-5
- Protect Your DMP from Unauthorized Management, page 9-4

Procedures

- Edit the Splash Screen Duration to Obscure the DMP IP Address, page 9-2
- Protect Your DMP from Unauthorized Management, page 9-4
- Manage and Edit Passwords, page 9-5
- Enable or Disable Types of Access to Your DMP, page 9-6
- Enable or Disable Centralized Management, page 9-7

Edit the Splash Screen Duration to Obscure the DMP IP Address

Timesaver **Complete this optional procedure at your discretion.**

You can change how long your DMP shows its splash screen during startup. This is useful when, for example, your organization prefers not to reveal an IP address casually to all observers.

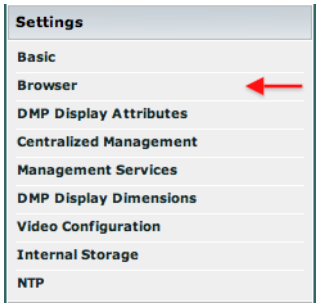
- A duration of 30,000 milliseconds (30 seconds) is the factory default.
- A duration of 1 millisecond turns off the splash screen.
- Any duration in the range from 2 to 5,000 milliseconds (5 seconds) does not have any effect.

Before You Begin

- Log in.

Procedure

Step 1 Click **Browser** in the Settings list.



Step 2 Enter a new duration in milliseconds in the **Splash Screen Display Time (in milliseconds)** field.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 5 Stop. You have completed this procedure.

Protect Your DMP from Unauthorized Management

Caution **Configure your network firewall to restrict access to DMPs over TCP port 7777.** Permit such access from only the DMM appliance where your fully licensed copy of *Cisco Digital Signs* is installed. If you do not know how to define an access control list (ACL), ask the security policy administrator for your network or see the manufacturer documentation for your firewall.

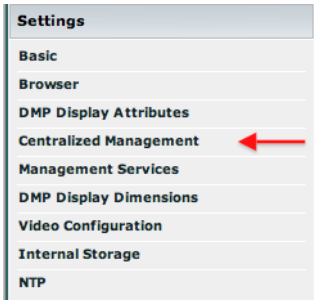
When you use *Cisco Digital Signs* to manage a network of DMPs centrally, you must configure each DMP to secure and trust its communication with *Cisco Digital Signs*.

Before You Begin

- Log in.

Procedure

Step 1 Click **Centralized Management** in the Settings list.



Step 2 Enter in the Digital Signs Server Timeout (sec) field the maximum number of seconds that your DMP should wait for a response from your DMM appliance.

Step 3 Enter the routable DMM appliance IP address or DNS-resolvable hostname in the **DMM Appliance IP Address** field.

Note **Has *Cisco Digital Signs* autodiscovered your new DMP?** If so, the DMM Appliance IP Address field might already be populated with the correct information for your DMM appliance.

Step 4 Click **Apply** to confirm and test your choices.

Your entries are recorded to volatile memory and take effect—but only until you change them or restart your DMP.

Step 5 When you are satisfied that you chose the correct settings, click **Save Configuration** in the Administration list, and then click **Save**.

Your entries take effect permanently and will persist even after your DMP restarts.

Note **Your DMM appliance and your DMP use HTTPS to communicate securely over TCP port 7777 when centralized management is enabled.**

Step 6 Stop. You have completed this procedure.

Related Topics

- Protect Your DMP from Unauthorized Management, page 9-4
- Log in, page 7-1

Manage and Edit Passwords

Note Until you change these passwords individually, they will be identical to the master password that you configured in the "Log in" section on page 7-1.

You can change them when they should differ. However, they will become identical again in the future if you edit the master password.

You can use DMPDM to change the DMP *Web Account* password and *Service Account* password on one DMP.

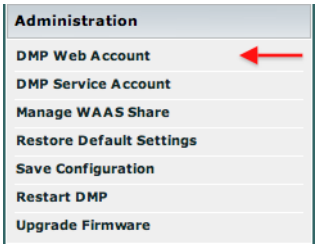
Before You Begin

- Log in.

Procedure

Step 1 Change the Web Account password.

a. Click **DMP Web Account** in the Administration list.

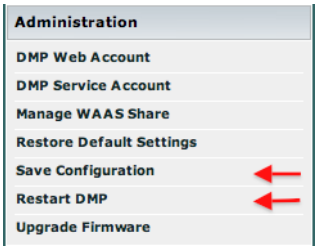


b. Enter your new password in the Password field and again in the Repeat Password field.

c. Click **Apply**.

d. Click **Save Configuration** in the Administration list, and then click **Save**.

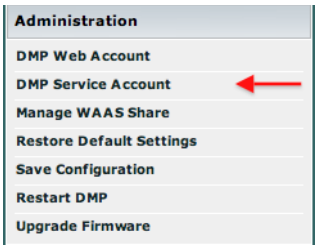
e. Click **Restart DMP** in the Administration list, and then click **Restart**.



Note **Because you changed the password, your trusted DMM appliance—if any—is prevented temporarily from communicating with this DMP.**

Step 2 Change the DMP Service Account password.

a. Click **DMP Service Account** in the Administration list.



b. Enter your new password in the Password field and again in the Repeat Password field.

c. Click **Apply**.

d. Click **Save Configuration** in the Administration list, and then click **Save**.

Step 3 (**Optional**) Is your DMP managed centrally? If so, repeat Step 3 in the "Protect Your DMP from Unauthorized Management" section on page 9-4.

Step 4 Stop. You have completed this procedure.

Proper communication is restored between your DMP and your trusted DMM appliance.

Enable or Disable Types of Access to Your DMP

You can enable or disable various kinds of administrative access to your DMP.

Procedure

Step 1 Click **Management Services** in the Settings list.

Step 2 Enter or edit the required values, and then click **Apply**.

Step 3 Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

Step 4 Restart your DMP.

Step 5 Stop. You have completed this procedure.

Related Topics

- Elements to Define Management Services, page 9-8
- Restart Your DMP, page 7-4

Enable or Disable Centralized Management

You can enable a remote DMM appliance to manage your DMP as part of a digital signage network.

Procedure

Step 1 Click **Centralized Management** in the Settings list.

Step 2 Enter or edit the required values.

Step 3 Click **Apply** to confirm that you are satisfied with the entries or changes that you made and to record them in volatile memory, .

After you click Apply, the entries or changes take effect. However, the previously defined values will return the next time that your DMP restarts.

Step 4 (**Optional**) *Would you like to put all changed values into effect permanently, so that they persist even after your DMP restarts?*

a. Choose **Administration > Save Configuration**.

b. Click **Save** when the Save Configuration page appears.

Step 5 Stop. You have completed this procedure.

Related Topics

- Elements to Define Centralized Management Settings, page 9-8

Reference

- SSL Encryption Ciphers That DMPs Support, page 9-7
- UI Reference Topics, page 9-8

SSL Encryption Ciphers That DMPs Support

DMPs support the following SSL ciphers in HTTPS connections.

- ADH-AES128-SHA
- ADH-AES256-SHA
- ADH-DES-CBC3-SHA
- AES128-SHA
- AES256-SHA
- DES-CBC-MD5
- DES-CBC-SHA
- DES-CBC3-MD5
- DES-CBC3-SHA
- DHE-DSS-AES128-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-DSS-DES-CBC3-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-RSA-DES-CBC3-SHA
- EXP-DES-CBC-SHA
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5
- IDEA-CBC-MD5
- IDEA-CBC-SHA
- RC2-CBC-MD5
- RC4-MD5
- RC4-SHA

UI Reference Topics

Elements to Define Centralized Management Settings

Table 9-1 Elements on the Centralized Management Page

Element	Description
Centralized Management	
DMM-DSM Server Timeout (in seconds)	The maximum number of seconds that your DMP will wait for a response from the DMM appliance that you identify in the DMM Host text box.
DMM Appliance IP Address	The routable IP address of the one DMM appliance that your DMP trusts. Alternatively, the DMP loopback IP address, 127.0.0.1.

Related Topics

- Enable or Disable Centralized Management, page 9-7

Elements to Define Management Services

Table 9-2 Elements on the Management Services Page

Element	Description
Management Services	
Enable Cisco TAC Troubleshooting Access	⚠ **Caution** We recommend that you assign a strong password to the Cisco TAC account and never reveal this password to anyone except your trusted support engineer after you open a support case with Cisco. Later, after your support case is closed, we recommend that you change the password. Indicates whether DMP login access is enabled or disabled for Cisco technical support staff. • **Enabled**—Your DMP allows Cisco technical support staff to log in. • **Disabled**—Your DMP *does not* allow Cisco technical support staff to log in. This feature is enabled by default but, in most cases, we do not support any use of this feature by anyone except a Cisco employee. **Note** This feature must be enabled during firmware upgrades.
Event Notifications	Indicates whether you enabled or disabled the feature to send event notification messages to one, trusted DMM appliance that you can choose. • **Enabled**—Your DMP sends notification messages. • **Disabled**—Your DMP *does not* send notification messages.

Table 9-2 Elements on the Management Services Page (continued)

Element	Description
FTP Server	Indicates whether you enabled or disabled the feature to run an FTP server and an SFTP server from your DMP. You might enable the FTP and SFTP services temporarily, for example, when you want to create a local copy on your DMP of an asset that you stored at a remote site. **Note** We recommend that you disable the FTP and SFTP services when you do not plan to use them.
Mount WAAS Share on Startup	Indicates whether your DMP will use the CIFS protocol to automatically mount the network share that you designated on the WAAS Share Settings page. • **On**—Upon starting, your DMP mounts the network share automatically. • **Off**—Upon starting, your DMP *does not* mount the network share automatically. **Note** DMPs can mount only one shared volume at a time.
TAC Account	
Password Repeat Password	The password for Cisco TAC to use while troubleshooting your DMP, if you chose Enabled from the Enable TAC Troubleshooting Access list. The password must contain at least 8 characters and, of these, at least one character must be an uppercase letter, at least one must be a lowercase letter, and at least one must be a numeral.

Related Topics

- Enable or Disable Types of Access to Your DMP, page 9-6
- Upgrade DMP Firmware, page 7-7
- Enable or Disable Centralized Management, page 9-7
- Mount or Unmount a Network Share, page 11-3

Elements to Define DMPDM Login Credentials

Table 9-3 Elements on the DMP Web Account Page

Element	Description
DMP Web Account	
User Name	The login name for DMPDM.
Password Repeat Password	The password that is associated with the DMPDM username. You must enter the password two times on the DMP Web Account page to confirm that you typed it correctly. The password must contain at least 8 characters and, of these, at least one character must be an uppercase letter, at least one must be a lowercase letter, and at least one must be a numeral.

Related Topics

- Manage and Edit Passwords, page 9-5

UI Reference: Elements to Define DMP Service Account (ftp and sftp) Login Credentials

Table 9-4 Elements on the DMP Service Account Page

Element	Description
FTP Server Account	
User Name	The login name for the DMP Service user account. The factory default is to use the login name **ftp**.
Password Repeat Password	The password that is associated with the DMP Service account login name. The factory default is to use the password **admin**, but we warned you to change it when you first set up your DMP. See the quick start guide for your DMP model type on Cisco.com. You must enter the password two times on the FTP Service Account page—one time apiece in each of these fields—to confirm that you typed it correctly. The password must contain at least 8 characters and, of these, at least one character must be an uppercase letter, at least one must be a lowercase letter, and at least one must be a numeral.

Related Topics

- Manage and Edit Passwords, page 9-5