Security Best Practices Supplement for Cisco Digital Media Encoders

Published: November 10, 2009

Revised: November 10, 2009

This supplement describes our recommendations about how to establish and maintain the most basic levels of security for these Cisco Digital Media Encoder models:

- DMS-DME 2200
- DMS-DME 2000
- DMS-DME 1100
- DMS-DME 1000

Warning **Factory-defined passwords exist by default on all new and newly restored DMEs. These credentials persist until you change them. Because they are well-known, these credentials are a security vulnerability in your network. Therefore, we recommend very strongly that you change them promptly each time that you start to configure a DME.**

In addition, some services are enabled by default that you might never use. We recommend that you disable all unneeded services.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Factory-Defined Login Credentials

Table 1-1 lists login credentials that are predefined on DMEs.

Table 1-1 Factory-Defined User Accounts and Passwords

Username	Password	DME Model				Notes
		DMS-DME 2200	DMS-DME 2000	DMS-DME 1100	DMS-DME 1000	
User Accounts for Microsoft Windows — *See Harden Windows, page 3.*						
GoStream	password[1]	—	—	—	X	**Warning** **Never configure a DME to log in automatically. Doing so prevents true security in your network.** If — despite our recommendation — you configure a DME to log into Windows automatically, password management becomes far more complex. Thus, any time that you neglect to change an auto-logon password specifically, you will prevent your DME from working as designed. See Other Required Password Maintenance (Only When Autologon Is Configured), page 5.
Niagara	password	X	X	X	—	
SCXUser	viewcast	X	X	X	X	Used for the Niagara SCX service as well as the web service. This is not the user account that is used to log-in to Niagara SCX.
User Accounts for the Niagara SCX Web Interface — *See Harden the web interface, page 4.*						
admin	admin	X	X	X	X	Used for the web-based administrative console on DMEs. Login is possible only through a system from which your DME is reachable. Its connection to your DME might be either direct or networked.

1. In 5.2.187 and later releases on a DME 1000.

Changing Factory-Defined Login Credentials

Warning **Be very careful as you complete this workflow. Any mistakes that you make might prevent your DME from booting correctly or functioning correctly.**

Before You Begin

- This workflow uses the instance of Microsoft Windows that runs on your DME. Even though a remote management connection might be sufficient, we recommend instead that you connect a keyboard, a mouse, and a monitor to your DME directly and use them to control Windows.
- From Step 1, this workflow assumes that your DME is either new or in a factory-restored condition. If this is not true, or if you are not sure, we recommend very strongly that you **perform a factory restore operation now**.

Procedure

	Task	Steps	Notes
Step 1	**Harden Windows** Change the Windows password for the main account.	a. Choose **Start > Settings > Control Panel > User Accounts**, and then: • If you have a DME 1000, choose **GoStream > Change my password**. • Otherwise, choose **Niagara > Change my password**. b. Change the password as desired. c. Click **Change Password**.	Depending on your DME model type, the username is either Niagara or GoStream. See Table 1-1 on page 2.
Step 2	**Harden Niagara SCX** Change the password for the SCXUser account, which you use to log in to Niagara SCX Encoder Explorer.	a. Choose **Start > Settings > Control Panel > User Accounts > SCXUser > Change my password**. b. Change the password as desired. c. Click **Change Password**.	—
Step 3	**Stop agent services**	a. Do either of the following: • Choose **Start > Run**. Type **system32** and press **Enter**. Double-click **GoStreamStopServices.bat**. • Choose **Start > All Programs > Viewcast > Niagara SCX > Niagara SCX Agent**, and then click **Stop**.	—

	Task	Steps	Notes
Step 4	**Update web.config to use the new password** Edit the web.config file.	**a.** Use Windows Explorer to browse to **\inetpub\wwwroot\encoderswebservice**. OR Browse instead to one of the following: • For a DMS-DME 1000, **\inetpub\wwwroot\GoStream**. • Otherwise, **\inetpub\wwwroot\Niagara**. **b.** Open the **web.config** file in a text editor, such as Notepad.exe. **c.** Locate the line of text that looks like this: `<identity impersonate="true" userName="scxuser" password="viewcast"/>` **d.** Edit the password string in this line of text. **e.** Save your work and exit the text editor.	—
Step 5	**Restart your DME**		—
Step 6	**Check for errors** Point the DME web browser at **http://localhost/encoderswebservice/**, and then verify that the SCX service is available.		—
Step 7	**Harden the web interface**	**a.** Point your browser to the HTTP address of your DME. **b.** Enter the username and the password, as prompted. The factory default for each of these is **admin**. **c.** Click **Log In**. **d.** Choose **Configuration > My NiagaraPro**. **e.** Click the username **admin** in the NiagaraPro Properties area. **f.** Enter the current password in the Password field. **g.** Enter the new password identically in both of these fields: • New Password • Confirm New Password **h.** Click **Change Password**. The changed password takes effect immediately.	—

Tip Saved changes are lost each time that you perform a factory restore operation. Remember to repeat this procedure any time that login credentials use factory-defined values.

What to Do Next

- If Windows is configured to allow automatic logins, see Other Required Password Maintenance (Only When Autologon Is Configured), page 5.
- Otherwise, see Tasks to Complete After Changing DME Login Passwords, page 6.

Other Required Password Maintenance (Only When Autologon Is Configured)

Warning **Never configure Microsoft Windows on your DME to enter login passwords automatically. Doing so creates a significant security vulnerability in your network.**

If you disregard the warning against allowing automatic logins and you configure them nonetheless, you must take additional steps to ensure that logins occur as expected after you change the encrypted auto-logon password that Windows uses.

Procedure

Step 1 Search the DME hard drive for *TweakUI.exe*. In most cases, this file is in F:\Windows.

Alternatively, you can download this file as part of a Microsoft tools package at http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx.

Step 2 Open **TweakUI**, and then choose **Logon > Autologon**.

Step 3 Click **Set Password**.

Step 4 Enter the new password twice, as prompted. Be careful that the password matches exactly.

Step 5 Click **OK** to save your work and exit TweakUI.

Step 6 Restart your DME.

Step 7 Verify that login occurs automatically and that the Windows desktop loads.

Note If you disregard the warning against allowing automatic logins and configure them nonetheless, ViewCast software will not work unless the Windows desktop loads correctly on your DME.

Tasks to Complete After Changing DME Login Passwords

Procedure

	Task	Notes
Step 1	Perform basic setup functions via the front panel.	See the "Basic Operation: Using the Front Panel" section in your DME user guide.
Step 2	Test and validate that your DME performs as expected.	**Tip** If your DME does not perform as expected, we recommend that you complete a factory restore operation. In this case, the factory-defined login credentials that you changed will become active again and might expose your network to attack or other types of unauthorized use.

Disabling Unneeded Services

Caution Intruders might use exposed services as security attack vectors against your network.

If your DME enables and exposes any service that is not required, you can disable it. Possible examples of such services include NNTP, SMTP, and SNMP.

Procedure

Step 1 Choose **Start > Programs > Administrative Tools > Services**.

Step 2 Double-click the name of a service that should be disabled.

Step 3 Click the **Log On** tab.

Step 4 Do one of the following:

- If only one hardware profile is listed, click it, and then click **Disable**.
- If multiple hardware profiles are listed, click one, then click **Disable**, and repeat as often as necessary until you have disabled this service on each profile.

Step 5 Click **Apply**, and then click **OK**.

Step 6 Restart Windows.

After a Live Event Is Finished, Remove Its Encoded Video Files from the DME File Share

Caution We strongly recommend that you save copies of the encoded video files on your DME file share, and then promptly delete the original files from your DME.

The file share uses a factory-default username and password, which you cannot change. Anyone who knows which network node is your DME and knows these login credentials can mount the file share and manipulate its files.

Learn More About...

To Learn About	Go To
Cisco DMS Components	
Cisco DMS products and technologies	http://cisco.com/go/dms
Cisco DMS technical documentation	http://cisco.com/go/dms/docroadmap
Cisco DMS MIB	http://cisco.com/go/dms/mib
Cisco DMS Services	
Cisco Academy of Digital Signage	http://cisco.com/go/dms/ads
Cisco Digital Media Creative Services	http://cisco.com/go/dms/services
Cisco	
Service contracts	http://cisco.com/go/cscc
Standard warranties	http://cisco.com/go/warranty [1]
Technical support	http://cisco.com/go/support
Technical documentation	http://cisco.com/go/techdocs
Product security	http://cisco.com/go/psirt
Sales	http://cisco.com/go/sales

Obtain Documentation or Submit a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

1. Then, for the device that *this guide* describes, click **Cisco 90-Day Limited Hardware Warranty Terms**