



# 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.**

---

- [Factory-Defined Login Credentials, page 2](#)
- [Changing Factory-Defined Login Credentials, page 3](#)
- [Other Required Password Maintenance \(Only When Autologon Is Configured\), page 5](#)
- [Tasks to Complete After Changing DME Login Passwords, page 6](#)
- [Disabling Unneeded Services, page 6](#)
- [After a Live Event Is Finished, Remove Its Encoded Video Files from the DME File Share, page 7](#)
- [Learn More About..., page 8](#)




---

**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	
<b>User Accounts for Microsoft Windows— See <a href="#">Harden Windows, page 3</a>.</b>						
GoStream	password <sup>1</sup>	—	—	—	X	 <b>Warning</b> 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 <a href="#">Other Required Password Maintenance (Only When Autologon Is Configured), page 5</a> .
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.
<b>User Accounts for the Niagara SCX Web Interface— See <a href="#">Harden the web interface, page 4</a>.</b>						
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	<b>Harden Windows</b> Change the Windows password for the main account.	<ol style="list-style-type: none"> <li>Choose <b>Start &gt; Settings &gt; Control Panel &gt; User Accounts</b>, and then:               <ul style="list-style-type: none"> <li>• If you have a DME 1000, choose <b>GoStream &gt; Change my password</b>.</li> <li>• Otherwise, choose <b>Niagara &gt; Change my password</b>.</li> </ul> </li> <li>Change the password as desired.</li> <li>Click <b>Change Password</b>.</li> </ol>	Depending on your DME model type, the username is either Niagara or GoStream. See <a href="#">Table 1-1 on page 2</a> .
Step 2	<b>Harden Niagara SCX</b> Change the password for the SCXUser account, which you use to log in to Niagara SCX Encoder Explorer.	<ol style="list-style-type: none"> <li>Choose <b>Start &gt; Settings &gt; Control Panel &gt; User Accounts &gt; SCXUser &gt; Change my password</b>.</li> <li>Change the password as desired.</li> <li>Click <b>Change Password</b>.</li> </ol>	—
Step 3	<b>Stop agent services</b>	<ol style="list-style-type: none"> <li>Do either of the following:               <ul style="list-style-type: none"> <li>• Choose <b>Start &gt; Run</b>. Type <b>system32</b> and press <b>Enter</b>. Double-click <b>GoStreamStopServices.bat</b>.</li> <li>• Choose <b>Start &gt; All Programs &gt; Viewcast &gt; Niagara SCX &gt; Niagara SCX Agent</b>, and then click <b>Stop</b>.</li> </ul> </li> </ol>	—

Task	Steps	Notes
<p><b>Step 4</b> <b>Update web.config to use the new password</b> Edit the web.config file.</p>	<p><b>a.</b> Use Windows Explorer to browse to <code>\inetpub\wwwroot\encoderswebservice</code>.</p> <p>OR</p> <p>Browse instead to one of the following:</p> <ul style="list-style-type: none"> <li>• For a DMS-DME 1000, <code>\inetpub\wwwroot\GoStream</code>.</li> <li>• Otherwise, <code>\inetpub\wwwroot\Niagara</code>.</li> </ul> <p><b>b.</b> Open the <b>web.config</b> file in a text editor, such as Notepad.exe.</p> <p><b>c.</b> Locate the line of text that looks like this:</p> <pre>&lt;identity impersonate="true"   userName="scxuser" password="viewcast"/&gt;</pre> <p><b>d.</b> Edit the password string in this line of text.</p> <p><b>e.</b> Save your work and exit the text editor.</p>	<p>—</p>
<p><b>Step 5</b> <b>Restart your DME</b></p>		<p>—</p>
<p><b>Step 6</b> <b>Check for errors</b> Point the DME web browser at <a href="http://localhost/encoderswebservice/">http://localhost/encoderswebservice/</a>, and then verify that the SCX service is available.</p>		<p>—</p>
<p><b>Step 7</b> <b>Harden the web interface</b></p>	<p><b>a.</b> Point your browser to the HTTP address of your DME.</p> <p><b>b.</b> Enter the username and the password, as prompted. The factory default for each of these is <b>admin</b>.</p> <p><b>c.</b> Click <b>Log In</b>.</p> <p><b>d.</b> Choose <b>Configuration &gt; My NiagaraPro</b>.</p> <p><b>e.</b> Click the username <b>admin</b> in the NiagaraPro Properties area.</p> <p><b>f.</b> Enter the current password in the Password field.</p> <p><b>g.</b> Enter the new password identically in both of these fields:</p> <ul style="list-style-type: none"> <li>• New Password</li> <li>• Confirm New Password</li> </ul> <p><b>h.</b> Click <b>Change Password</b>.</p> <p>The changed password takes effect immediately.</p>	<p>—</p>



**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**

	<b>Task</b>	<b>Notes</b>
<b>Step 1</b>	Perform basic setup functions via the front panel.	See the “Basic Operation: Using the Front Panel” section in your DME user guide.
<b>Step 2</b>	Test and validate that your DME performs as expected.	<b>Tip</b> 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
<b>Cisco DMS Components</b>	
Cisco DMS products and technologies	<a href="http://cisco.com/go/dms">http://cisco.com/go/dms</a>
Cisco DMS technical documentation	<a href="http://cisco.com/go/dms/docroadmap">http://cisco.com/go/dms/docroadmap</a>
Cisco DMS MIB	<a href="http://cisco.com/go/dms/mib">http://cisco.com/go/dms/mib</a>
<b>Cisco DMS Services</b>	
Cisco Academy of Digital Signage	<a href="http://cisco.com/go/dms/ads">http://cisco.com/go/dms/ads</a>
Cisco Digital Media Creative Services	<a href="http://cisco.com/go/dms/services">http://cisco.com/go/dms/services</a>
<b>Cisco</b>	
Service contracts	<a href="http://cisco.com/go/csc">http://cisco.com/go/csc</a>
Standard warranties	<a href="http://cisco.com/go/warranty">http://cisco.com/go/warranty</a> <sup>1</sup>
Technical support	<a href="http://cisco.com/go/support">http://cisco.com/go/support</a>
Technical documentation	<a href="http://cisco.com/go/techdocs">http://cisco.com/go/techdocs</a>
Product security	<a href="http://cisco.com/go/psirt">http://cisco.com/go/psirt</a>
Sales	<a href="http://cisco.com/go/sales">http://cisco.com/go/sales</a>

## 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**

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopied, recorded, or otherwise without prior written permission from Cisco Systems, Inc. ViewCast<sup>®</sup>, the ViewCast logo, Niagara<sup>®</sup>, the Niagara logo, GoStream, Niagara SCX<sup>®</sup>, EZ Stream and SimulStream<sup>®</sup> and Osprey<sup>®</sup> are trademarks or registered trademarks of ViewCast Corporation or its



subsidiaries. Macintosh® is a registered trademark of Apple Computer, Inc. Microsoft®, Windows®, Windows® XP, Windows Media® and DirectDraw® are registered trademarks of Microsoft Corporation. Linux® is a registered trademark of Linus Torvalds. RealNetworks®, RealAudio®, RealVideo®, RealMedia®, RealPlayer®, RealProducer®, Helix® and SureStream are the trademarks or registered trademarks of RealNetworks, Inc. Flash® is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries. Intel® is a registered trademark of Intel Corporation. Indeo® is a registered trademark of Ligos Corporation.

© 2009 Cisco Systems, Inc. All rights reserved.

