



# Release Notes for Cisco ACNS Software, Release 5.0.11

---

February 27, 2004



**Note**

---

The most current Cisco documentation for released products is available at Cisco.com at <http://www.cisco.com>. The online documents may contain updates and modifications made after the hardcopy documents were printed.

---

## Documentation Survey

Is Cisco documentation helpful? Click [here](#) to give us your feedback.

## Contents

These release notes contain information about ACNS software, Release 5.0.11. These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Important Notes, page 2](#)
- [Caveats, page 3](#)
- [Related Documentation, page 38](#)
- [Obtaining Documentation, page 39](#)
- [Documentation Feedback, page 39](#)
- [Obtaining Technical Assistance, page 40](#)
- [Obtaining Additional Publications and Information, page 41](#)



---

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

# Introduction

These release notes describe supported hardware and open and resolved caveats regarding ACNS software, Release 5.0.11.

## System Requirements

The following section lists the hardware platforms that can run ACNS software.

## Hardware Supported

ACNS software, Release 5.0.11 supports the following hardware platforms:

- NM-CE-BP-SCSI
- NM-CE-BP-20G
- NM-CE-BP-40G
- CDM-4630
- CDM-4650
- CE-7320
- CR-4430
- CE-590
- CE-590-DC
- CE-560
- CE-560AV
- CE-507
- CE-507AV
- CE-510-K9
- CE-565-K9
- CE-7325-K9
- CE-7305-K9

## Important Notes

This section emphasizes important information regarding ACNS 5.0.x software.

## Media File System Issues When Downgrading to ACNS 5.0 Software

If you have configured the media file system (mediafs) with ACNS 5.1 software or later, and then downgrade to ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to ACNS network file system (cdnfs) disk space. (The mediafs is used for on-demand content that is fetched through the two streaming protocols [RTSP and WMT]. The cdnfs is used for pre-positioned content in the ACNS network.)

This situation occurs because of a design change that was implemented in ACNS 5.1 software. Because ACNS 5.0 software is not compatible with this change, the disk space becomes assigned to cdnfs instead of mediafs. To work around this problem, follow these steps:

1. After you downgrade to ACNS 5.0 software, use the CLI (**disk config EXEC** command) or the GUI to assign the mediafs disk space.

Use the Content Distribution Manager GUI for Content Engines that are registered with a Content Distribution Manager. Use the Content Engine GUI for standalone Content Engines (that is, Content Engines that are not registered with a Content Distribution Manager and are being managed through the Content Engine GUI or CLI).

2. Reboot the Content Engine for the disk configuration changes to take effect.

## WebSense Issues When Downgrading to ACNS 5.0 Software or ACNS 5.1 Software

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. Note that the ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed.

To avoid this problem when downgrading from ACNS 5.2.x software to ACNS software 5.1 or ACNS 5.0 software, follow these steps:

1. Disable the local (internal) Websense server on the Content Engine.
2. Deactivate the Websense services on the Content Engine.
3. Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.

## Caveats

This section lists and describes caveats that are open in ACNS software, Release 5.0.11. Caveats describe unexpected behavior in ACNS software, Release 5.0.11. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

### Open Caveats - ACNS Software, Release 5.0.11

- CSCdy02581

Symptom: WCCP bypass does not function properly when bypassing large packets from the client. Therefore, the client never receives an acknowledgment from the server for the data sent.

Condition: This problem occurs when the Content Engine bypasses the connection and the server advertises a maximum segment size (MSS) of 1460 bytes.

Workaround: If the client's path is configured to discover the maximum transmission unit (MTU), users can configure a lower value of MTU on the router interface connected to the Content Engine. Thus, if a client sent a large packet, the router drops it and sends an Internet Control Message Protocol (ICMP) message with the reduced MTU value. Clients can then adjust to the lower value.

- CSCdy82311

Symptom: Content cannot be acquired using strong authentication from secure origin servers that use certificates from nonstandard certificate authorities (CAs). If strong authentication was chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log will contain the following error message:

```
Strong Cert Authentication rejects certificate due to error: ssl error code
```

Condition: This problem occurs if the origin server uses a certificate that is not recognized as a standard certificate by the ACNS acquirer. For content acquisition from secure sites over HTTPS using strong authentication, only sites with certificates from standard certificate authorities are supported.




---

**Note** With strong authentication, if there are any errors during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors (for example, errors such as certificate has expired, certificate is not yet valid, and subject issuer mismatch) are allowed during certificate verification.

---

Workaround: Use one of these workarounds:

- Use weak authentication.
- On the secure server, use a certificate that was generated by one of the standard certificate authorities. ACNS network administrators should refer to the following information to determine which CA certificate they should install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.0.11 software release, refer to the following certificate list:

```
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
    Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After : Aug  1 23:59:59 2028 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification
    Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert
    Class 3 Policy Validation Authority,
    CN=http://www.valicert.com//Email=info@valicert.com
    Validity
        Not Before: Jun 26 00:22:33 1999 GMT
        Not After : Jun 26 00:22:33 2019 GMT
    Subject: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert
    Class 3 Policy Validation Authority,
    CN=http://www.valicert.com//Email=info@valicert.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, L=Brussels, O=BelSign NV, OU=BelSign Object Publishing
    Certificate Authority, CN=BelSign Object Publishing CA/Email=webmaster@belsign.be
    Validity
        Not Before: Sep 19 22:03:00 1997 GMT
        Not After : Sep 19 22:03:00 2007 GMT
    Subject: C=BE, L=Brussels, O=BelSign NV, OU=BelSign Object Publishing
    Certificate Authority, CN=BelSign Object Publishing CA/Email=webmaster@belsign.be
-----END CERTIFICATE-----
```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Equifax Secure, OU=Equifax Secure eBusiness CA-2
    Validity
        Not Before: Jun 23 12:14:45 1999 GMT
        Not After : Jun 23 12:14:45 2019 GMT
    Subject: C=US, O=Equifax Secure, OU=Equifax Secure eBusiness CA-2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999
    VeriSign, Inc. - For authorized use only, CN=VeriSign Class 4 Public Primary
    Certification Authority - G3
    Validity
        Not Before: Oct  1 00:00:00 1999 GMT
        Not After : Jul 16 23:59:59 2036 GMT
    Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c)
    1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 4 Public Primary
    Certification Authority - G3
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=CA, ST=ON, L=Toronto, O=CertEngine Inc., OU=Certification
    Authority Division, CN=certengine/Email=ca@certengine.com
    Validity
        Not Before: Jan  1 00:00:00 1998 GMT
        Not After : Jan 17 00:00:00 2038 GMT
    Subject: C=CA, ST=ON, L=Toronto, O=CertEngine Inc., OU=Certification
    Authority Division, CN=certengine/Email=ca@certengine.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Code
    Signing Root
    Validity
        Not Before: May 17 14:01:00 2000 GMT
        Not After : May 17 23:59:00 2025 GMT
    Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust
    Code Signing Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=United States Postal Service, OU=www.usps.com/CPS,
    CN=USPS Root CA Validity
        Not Before: Aug 16 21:06:39 2000 GMT
        Not After : Aug 15 13:06:25 2020 GMT
    Subject: C=US, O=United States Postal Service, OU=www.usps.com/CPS,
    CN=USPS Production CA 1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Equifax, OU=Equifax Secure Certificate Authority
    Validity
        Not Before: Aug 22 16:41:51 1998 GMT
        Not After : Aug 22 16:41:51 2018 GMT
    Subject: C=US, O=Equifax, OU=Equifax Secure Certificate Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=DE, O=Deutsche Telekom AG, OU=TeleSec Trust Center,
CN=Deutsche Telekom Root CA
    Validity
        Not Before: Dec  9 09:11:00 1998 GMT
        Not After  : Dec  9 23:59:00 2004 GMT
    Subject: C=DE, O=Deutsche Telekom AG, OU=TeleSec Trust Center,
CN=Deutsche Telekom Root CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
Provider, CN=BNL Corporate Certification/Email=key_management@bnl.it
    Validity
        Not Before: Aug 11 14:43:19 2000 GMT
        Not After  : Aug 10 14:43:19 2005 GMT
    Subject: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
Provider, CN=BNL Corporate Certification/Email=key_management@bnl.it
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VISA, OU=Visa International Service Association, CN=GP
Root 3
    Validity
        Not Before: Aug 16 23:34:00 2000 GMT
        Not After  : Aug 15 23:59:00 2020 GMT
    Subject: C=US, O=VISA, OU=Visa International Service Association,
CN=GP Root 3
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co.,
OU=National Retail Federation, CN=DST (NRF) RootCA/Email=ca@digsigtrust.com
    Validity
        Not Before: Dec 11 16:14:16 1998 GMT
        Not After  : Dec  8 16:14:16 2008 GMT
    Subject: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co.,
OU=National Retail Federation, CN=DST (NRF) RootCA/Email=ca@digsigtrust.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Commercial Certification
Authority
    Validity
        Not Before: Nov  4 18:58:34 1994 GMT
        Not After  : Nov  3 18:58:34 1999 GMT
    Subject: C=US, O=RSA Data Security, Inc., OU=Commercial Certification
Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
    Validity
        Not Before: May 18 00:00:00 1998 GMT
        Not After  : Aug  1 23:59:59 2028 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
    Validity
        Not Before: Sep 15 12:00:00 1998 GMT
        Not After  : Jan 28 12:00:00 2009 GMT
    Subject: C=BE, O=GlobalSign nv-sa, OU=Primary Class 1 CA,
CN=GlobalSign Primary Class 1 CA
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
    OU=Certification Services Division, CN=Thawte Personal Freemail CA/Email=personal-
    freemail@thawte.com
    Validity
        Not Before: Aug 30 00:00:00 2000 GMT
        Not After : Aug 27 23:59:59 2004 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte, OU=Certificate
    Services, CN=Personal Freemail RSA 2000.8.30
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VISA, OU=Visa International Service Association, CN=GP
    Root 5
    Validity
        Not Before: Aug 17 00:28:00 2000 GMT
        Not After : Aug 16 23:59:00 2020 GMT
    Subject: C=US, O=VISA, OU=Visa International Service Association,
    CN=GP Root 5
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=United States Postal Service, OU=www.usps.com/CPS,
    CN=USPS Root CA
    Validity
        Not Before: Aug 15 19:35:58 2000 GMT
        Not After : Aug 15 19:35:58 2020 GMT
    Subject: C=US, O=United States Postal Service, OU=www.usps.com/CPS,
    CN=USPS Root CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
    OU=Certification Services Division, CN=Thawte Personal Premium
    CA/Email=personal-premium@thawte.com
    Validity
        Not Before: Jan  1 00:00:00 1996 GMT
        Not After : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
    OU=Certification Services Division, CN=Thawte Personal Premium CA/Email=personal-
    premium@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=Xcert International Inc., OU=Xcert Root CA v1 1024
    Validity
        Not Before: Aug 18 18:50:56 2000 GMT
        Not After : Aug 15 19:01:08 2025 GMT
    Subject: O=Xcert International Inc., OU=Xcert Root CA v1 1024
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=CA, ST=ON, L=Toronto, O=BankEngine Inc., OU=Certification
    Authority Division, CN=bankengine/Email=ca@bankengine.com
    Validity
        Not Before: Jan  1 00:00:00 1998 GMT
        Not After : Jan 17 00:00:00 2038 GMT
    Subject: C=CA, ST=ON, L=Toronto, O=BankEngine Inc., OU=Certification
    Authority Division, CN=bankengine/Email=ca@bankengine.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, L=Brussels, O=BelSign NV, OU=BelSign Secure Server
    Certificate Authority, CN=BelSign Secure Server CA/Email=webmaster@belsign.be
    Validity
        Not Before: Jul 16 22:00:54 1997 GMT
        Not After : Jul 16 22:00:54 2007 GMT
    Subject: C=BE, L=Brussels, O=BelSign NV, OU=BelSign Secure Server
    Certificate Authority, CN=BelSign Secure Server CA/Email=webmaster@belsign.be
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, ST=Utah, L=Salt Lake City, O=Xcert EZ by DST, CN=Xcert
EZ by DST/Email=ca@digsigtrust.com
    Validity
        Not Before: Jul 14 16:14:18 1999 GMT
        Not After : Jul 11 16:14:18 2009 GMT
    Subject: C=US, ST=Utah, L=Salt Lake City, O=Xcert EZ by DST, CN=Xcert
EZ by DST/Email=ca@digsigtrust.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Entrust.net, OU=www.entrust.net/Client_CA_Info/CPS
incorp. by ref. limits liab., OU=(c) 1999 Entrust.net Limited, CN=Entrust.net
Client Certification Authority
    Validity
        Not Before: Oct 12 19:24:30 1999 GMT
        Not After : Oct 12 19:54:30 2019 GMT
    Subject: C=US, O=Entrust.net, OU=www.entrust.net/Client_CA_Info/CPS
incorp. by ref. limits liab., OU=(c) 1999 Entrust.net Limited, CN=Entrust.net
Client Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=American Express Company, Inc., OU=American Express
Technologies, CN=American Express Global Certificate Authority
    Validity
        Not Before: Aug 14 19:06:00 1998 GMT
        Not After : Aug 14 23:59:00 2013 GMT
    Subject: C=US, O=American Express Company, Inc., OU=American Express
Technologies, CN=American Express Global Certificate Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Equifax, OU=Equifax Premium Certificate Authority
    Validity
        Not Before: Aug 24 22:54:23 1998 GMT
        Not After : Aug 24 22:54:23 2018 GMT
    Subject: C=US, O=Equifax, OU=Equifax Premium Certificate Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
Services Division, CN=Thawte Server CA/Email=server-certs@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
Services Division, CN=Thawte Server CA/Email=server-certs@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=Xcert International Inc., OU=Xcert Root CA v1
    Validity
        Not Before: Aug 18 18:40:50 2000 GMT
        Not After : Aug 15 19:00:38 2025 GMT
    Subject: O=Xcert International Inc., OU=Xcert Root CA v1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co.,
OU=DSTCA X2,
CN=DST RootCA X2/Email=ca@digsigtrust.com
    Validity
        Not Before: Nov 30 22:46:16 1998 GMT
        Not After : Nov 27 22:46:16 2008 GMT

```

```

Subject: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co.,
OU=DSTCA X2,
CN=DST RootCA X2/Email=ca@digsigtrust.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Issuer: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
Provider, CN=BNL SSL Certification/Email=key_management@bnl.it
Validity
Not Before: Aug 11 14:41:14 2000 GMT
Not After : Aug 10 14:41:14 2005 GMT
Subject: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
Provider, CN=BNL SSL Certification/Email=key_management@bnl.it
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999
VeriSign, Inc.- For authorized use only, CN=VeriSign Class 2 Public Primary
Certification Authority - G3
Validity
Not Before: Oct 1 00:00:00 1999 GMT
Not After : Jul 16 23:59:59 2036 GMT
Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c)
1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 2 Public Primary
Certification Authority - G3
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Issuer: C=WW, O=beTRUSTed, CN=beTRUSTed Root CAs, CN=beTRUSTed Root CA
Validity
Not Before: Jun 20 14:21:04 2000 GMT
Not After : Jun 20 13:21:04 2010 GMT
Subject: C=WW, O=beTRUSTed, CN=beTRUSTed Root CAs, CN=beTRUSTed Root CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification
Authority
Validity
Not Before: Aug 4 00:00:00 2000 GMT
Not After : Aug 3 23:59:59 2004 GMT
Subject: O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use
at https://www.verisign.com/RPA (c)00, CN=Class 1 Public Primary OCSP Responder
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
Data Networks GmbH, OU=TC TrustCenter Class 3 CA/Email=certificate@trustcenter.de
Validity
Not Before: Mar 9 13:58:49 1998 GMT
Not After : Dec 31 13:58:49 2005 GMT
Subject: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
Data Networks GmbH, OU=TC TrustCenter Class 3 CA/Email=certificate@trustcenter.de
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification
Authority
Validity
Not Before: Jan 29 00:00:00 1996 GMT
Not After : Aug 1 23:59:59 2028 GMT
Subject: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Mobile
Root
    Validity
        Not Before: May 12 18:20:00 2000 GMT
        Not After : May 12 23:59:00 2020 GMT
    Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Mobile
Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
    Validity
        Not Before: May 18 00:00:00 1998 GMT
        Not After : May 18 23:59:59 2018 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Digital Signature Trust Co., OU=DSTCA E2
    Validity
        Not Before: Dec  9 19:17:26 1998 GMT
        Not After : Dec  9 19:47:26 2018 GMT
    Subject: C=US, O=Digital Signature Trust Co., OU=DSTCA E2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Premium Server
CA/Email=premium-server@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
    Services Division, CN=Thawte Premium Server CA/Email=premium-server@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Entrust.net, OU=www.entrust.net/CPS incorp. by ref.
(limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Secure Server
Certification Authority
    Validity
        Not Before: May 25 16:09:40 1999 GMT
        Not After : May 25 16:39:40 2019 GMT
    Subject: C=US, O=Entrust.net, OU=www.entrust.net/CPS incorp. by ref.
(limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Secure Server
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust
Public CA Root
    Validity
        Not Before: May 30 10:41:50 2000 GMT
        Not After : May 30 10:41:50 2020 GMT
    Subject: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Public
CA Root
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure eBusiness CA-1
    Validity
        Not Before: Jun 21 04:00:00 1999 GMT
        Not After : Jun 21 04:00:00 2020 GMT
    Subject: C=US, O=Equifax Secure Inc., CN=Equifax Secure eBusiness CA-1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=CA, ST=ON, L=Toronto, O=TraderEngine Inc., OU=Certification
    Authority Division, CN=traderengine/Email=ca@traderengine.com
    Validity
        Not Before: Jan  1 00:00:00 1998 GMT
        Not After : Jan 17 00:00:00 2038 GMT
    Subject: C=CA, ST=ON, L=Toronto, O=TraderEngine Inc., OU=Certification
    Authority Division, CN=traderengine/Email=ca@traderengine.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust
    Qualified CA Root
    Validity
        Not Before: May 30 10:44:50 2000 GMT
        Not After : May 30 10:44:50 2020 GMT
    Subject: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust
    Qualified CA Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Digital Signature Trust Co., OU=DSTCA E1
    Validity
        Not Before: Dec 10 18:10:23 1998 GMT
        Not After : Dec 10 18:40:23 2018 GMT
    Subject: C=US, O=Digital Signature Trust Co., OU=DSTCA E1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
    Provider, CN=BBTOPT
    RADE Certification/Email=key_management@bnl.it
    Validity
        Not Before: Aug 11 14:52:07 2000 GMT
        Not After : Aug 10 14:52:07 2005 GMT
    Subject: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
    Provider, CN=BBTOP TRADE Certification/Email=key_management@bnl.it
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=Xcert International Inc., OU=Xcert Root CA 1024
    Validity
        Not Before: Aug 18 18:31:32 2000 GMT
        Not After : Aug 15 19:00:56 2025 GMT
    Subject: O=Xcert International Inc., OU=Xcert Root CA 1024
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification
    Authority
    Validity
        Not Before: Aug  4 00:00:00 2000 GMT
        Not After : Aug  3 23:59:59 2004 GMT
    Subject: O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use
    at https://www.verisign.com/RPA (c)00, CN=Class 3 Public Primary OCSP Responder
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust Global Root
    Validity
        Not Before: Aug 13 00:29:00 1998 GMT
        Not After  : Aug 13 23:59:00 2018 GMT
    Subject: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust Global Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust
    Root 3
    Validity
        Not Before: Aug 10 19:59:08 1998 GMT
        Not After  : Aug 10 19:36:39 2008 GMT
    Subject: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust Root 3
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=JP, O=CyberTrust Japan, Inc., CN=CyberTrust JAPAN Secure
Server CA
    Validity
        Not Before: Aug  4 08:06:32 1998 GMT
        Not After  : Aug  4 23:59:00 2003 GMT
    Subject: C=JP, O=CyberTrust Japan, Inc., CN=CyberTrust JAPAN Secure
Server CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
Provider, CN=BNL Professional Certification/Email=key_management@bnl.it
    Validity
        Not Before: Aug 11 14:45:06 2000 GMT
        Not After  : Aug 10 14:45:06 2005 GMT
    Subject: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
Provider, CN=BNL Professional Certification/Email=key_management@bnl.it
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
    Validity
        Not Before: Aug  4 00:00:00 2000 GMT
        Not After  : Aug  3 23:59:59 2004 GMT
    Subject: O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use
at https://www.verisign.com/RPA (c)00, CN=Secure Server OCSP Responder
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 4 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 1999 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 4 Public Primary Certification
Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust
    Root 5
    Validity
        Not Before: Aug 14 14:50:00 1998 GMT
        Not After : Aug 14 23:59:00 2013 GMT
    Subject: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust Root 5
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert
Class 1 Policy Validation Authority,
CN=http://www.valicert.com//Email=info@valicert.com
    Validity
        Not Before: Jun 25 22:23:48 1999 GMT
        Not After : Jun 25 22:23:48 2019 GMT
    Subject: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert
Class 1 Policy Validation Authority,
CN=http://www.valicert.com//Email=info@valicert.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=JP, O=CyberTrust Japan, Inc., CN=CyberTrust JAPAN Root CA
    Validity
        Not Before: Aug  4 07:57:00 1998 GMT
        Not After : Aug  4 23:59:00 2003 GMT
    Subject: C=JP, O=CyberTrust Japan, Inc., CN=CyberTrust JAPAN Root CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
Data Networks GmbH, OU=TC TrustCenter Class 0 CA/Email=certificate@trustcenter.de
    Validity
        Not Before: Mar  9 13:54:48 1998 GMT
        Not After : Dec 31 13:54:48 2005 GMT
    Subject: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
Data Networks GmbH, OU=TC TrustCenter Class 0 CA/Email=certificate@trustcenter.de
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
    Validity
        Not Before: May 18 00:00:00 1998 GMT
        Not After : Aug  1 23:59:59 2028 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use
only, OU=VeriSign Trust Network
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=Thawte, OU=Thawte Universal CA Root, CN=Thawte Universal CA
Root
    Validity
        Not Before: Dec  5 13:56:05 1999 GMT
        Not After : Apr  3 13:56:05 2037 GMT
    Subject: O=Thawte, OU=Thawte Universal CA Root, CN=Thawte Universal CA
Root
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: O=Entrust.net, OU=www.entrust.net/CPS_2048 incorp. by ref.
    (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification
    Authority (2048)
    Validity
        Not Before: Dec 24 17:50:51 1999 GMT
        Not After : Dec 24 18:20:51 2019 GMT
    Subject: O=Entrust.net, OU=www.entrust.net/CPS_2048 incorp. by ref.
    (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification
    Authority (2048)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=GTE Corporation, CN=GTE CyberTrust Root
    Validity
        Not Before: Feb 23 23:01:00 1996 GMT
        Not After : Feb 23 23:59:00 2006 GMT
    Subject: C=US, O=GTE Corporation, CN=GTE CyberTrust Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999
    VeriSign, Inc.- For authorized use only, CN=VeriSign Class 1 Public Primary
    Certification Authority - G3
    Validity
        Not Before: Oct  1 00:00:00 1999 GMT
        Not After : Jul 16 23:59:59 2036 GMT
    Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c)
    1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 1 Public Primary
    Certification Authority - G3
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
    Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use
    only, OU=VeriSign Trust Network
    Validity
        Not Before: May 18 00:00:00 1998 GMT
        Not After : Aug  1 23:59:59 2028 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
    Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use
    only, OU=VeriSign Trust Network
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE
    CyberTrust Root 2
    Validity
        Not Before: Aug 11 11:35:07 1998 GMT
        Not After : Aug 11 11:22:16 2008 GMT
    Subject: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
    CN=GTE CyberTrust Root 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
    Data Networks GmbH, OU=TC TrustCenter Class 1 CA/Email=certificate@trustcenter.de
    Validity
        Not Before: Mar  9 13:56:33 1998 GMT
        Not After : Dec 31 13:56:33 2005 GMT
    Subject: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
    Data Networks GmbH, OU=TC TrustCenter Class 1 CA/Email=certificate@trustcenter.de
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999
VeriSign, Inc.- For authorized use only, CN=VeriSign Class 3 Public Primary
Certification Authority - G3
    Validity
        Not Before: Oct  1 00:00:00 1999 GMT
        Not After  : Jul 16 23:59:59 2036 GMT
    Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c)
1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary
Certification Authority - G3
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification
Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Aug  1 23:59:59 2028 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification
Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 4 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
    Validity
        Not Before: May 18 00:00:00 1998 GMT
        Not After  : Aug  1 23:59:59 2028 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 4 Public Primary Certification
Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign
Trust Network
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
    Validity
        Not Before: Sep  1 12:00:00 1998 GMT
        Not After  : Jan 28 12:00:00 2014 GMT
    Subject: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=Xcert International Inc., OU=Xcert Root CA
    Validity
        Not Before: Aug 18 18:18:17 2000 GMT
        Not After  : Aug 15 19:03:17 2025 GMT
    Subject: O=Xcert International Inc., OU=Xcert Root CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
    Validity
        Not Before: Jan 28 12:00:00 1999 GMT
        Not After  : Jan 28 12:00:00 2009 GMT
    Subject: C=BE, O=GlobalSign nv-sa, OU=Primary Class 3 CA,
CN=GlobalSign Primary Class 3 CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=Class 1
Validation Authority - OCSP, CN=http://www.valicert.net//Email=info@valicert.com
    Validity
        Not Before: Feb 12 11:50:05 2000 GMT
        Not After  : Feb 10 11:50:05 2005 GMT
    Subject: L=ValiCert Validation Network, O=ValiCert, Inc., OU=Class 1
Validation Authority - OCSP, CN=http://www.valicert.net//Email=info@valicert.com
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
    Provider, CN=Multicertify/Email=key_management@bnl.it
    Validity
        Not Before: Aug 11 14:49:51 2000 GMT
        Not After : Aug 10 14:49:51 2005 GMT
    Subject: C=IT, O=BNL Multiservizi S.p.A., OU=Certification Service
    Provider, CN=Multicertify/Email=key_management@bnl.it
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
    Data Networks GmbH, OU=TC TrustCenter Class 2 CA/Email=certificate@trustcenter.de
    Validity
        Not Before: Mar  9 13:57:44 1998 GMT
        Not After : Dec 31 13:57:44 2005 GMT
    Subject: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
    Data Networks GmbH, OU=TC TrustCenter Class 2 CA/Email=certificate@trustcenter.de
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
    Validity
        Not Before: Jan 28 12:00:00 1999 GMT
        Not After : Jan 28 12:00:00 2009 GMT
    Subject: C=BE, O=GlobalSign nv-sa, OU=Primary Class 2 CA,
    CN=GlobalSign Primary Class 2 CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Digital Signature Trust Co., OU=DST (ANX Network) CA
    Validity
        Not Before: Dec  9 15:46:48 1998 GMT
        Not After : Dec  9 16:16:48 2018 GMT
    Subject: C=US, O=Digital Signature Trust Co., OU=DST (ANX Network) CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust
    Class 1 CA Root
    Validity
        Not Before: May 30 10:38:31 2000 GMT
        Not After : May 30 10:38:31 2020 GMT
    Subject: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust
    Class 1 CA Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VISA, OU=Visa International Service Association
    Validity
        Not Before: Aug 16 21:52:00 2000 GMT
        Not After : Aug 15 23:59:00 2020 GMT
    Subject: C=US, O=VISA, OU=Visa International Service Association
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
    Certification Authority
    Validity
        Not Before: Aug  1 00:00:00 2000 GMT
        Not After : Jul 31 23:59:59 2004 GMT
    Subject: O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use
    at https://www.verisign.com/RPA (c)00, CN=Class 2 Public Primary OCSP Responder
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
    OU=Certification Services Division, CN=Thawte Personal Freemail CA/Email=personal-freemail@thawte.com
    Validity
        Not Before: Jan  1 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
    OU=Certification Services Division, CN=Thawte Personal Freemail
    CA/Email=personal-freemail@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
    Validity
        Not Before: May 12 18:46:00 2000 GMT
        Not After  : May 12 23:59:00 2025 GMT
    Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness
    CA-1
    Validity
        Not Before: Jun 21 04:00:00 1999 GMT
        Not After  : Jun 21 04:00:00 2020 GMT
    Subject: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global
    eBusiness CA-1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
    Data Networks GmbH, OU=TC TrustCenter Class 4 CA/Email=certificate@trustcenter.de
    Validity
        Not Before: Mar  9 14:00:20 1998 GMT
        Not After  : Dec 31 14:00:20 2005 GMT
    Subject: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in
    Data Networks GmbH, OU=TC TrustCenter Class 4 CA/Email=certificate@trustcenter.de
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert
    Class 2 Policy Validation Authority,
    CN=http://www.valicert.com//Email=info@valicert.com
    Validity
        Not Before: Jun 26 00:19:54 1999 GMT
        Not After  : Jun 26 00:19:54 2019 GMT
    Subject: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert
    Class 2 Policy Validation Authority,
    CN=http://www.valicert.com//Email=info@valicert.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=CA, ST=ON, L=Toronto, O=MailEngine Inc., OU=Certification
    Authority Division, CN=mailengine/Email=ca@mailengine.com
    Validity
        Not Before: Jan  1 00:00:00 1998 GMT
        Not After  : Jan 17 00:00:00 2038 GMT
    Subject: C=CA, ST=ON, L=Toronto, O=MailEngine Inc., OU=Certification
    Authority Division, CN=mailengine/Email=ca@mailengine.com
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
    Validity
        Not Before: Nov  9 00:00:00 1994 GMT
        Not After  : Jan  7 23:59:59 2010 GMT
    Subject: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
OU=Certification Services Division, CN=Thawte Personal Basic
CA/Email=personal-basic@thawte.com
    Validity
        Not Before: Jan  1 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting,
OU=Certification Services Division, CN=Thawte Personal Basic
CA/Email=personal-basic@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
    Validity
        Not Before: Jan 28 12:00:00 1999 GMT
        Not After  : Jan 28 12:00:00 2009 GMT
    Subject: C=BE, O=GlobalSign nv-sa, OU=Partners CA, CN=GlobalSign
Partners CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust
Co., OU=United Parcel Service, CN=DST (UPS) RootCA/Email=ca@digsigtrust.com
    Validity
        Not Before: Dec 10 00:25:46 1998 GMT
        Not After  : Dec  7 00:25:46 2008 GMT
    Subject: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust
Co., OU=United Parcel Service, CN=DST (UPS) RootCA/Email=ca@digsigtrust.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VISA, OU=Visa International Service Association, CN=GP
Root 2
    Validity
        Not Before: Aug 16 22:51:00 2000 GMT
        Not After  : Aug 15 23:59:00 2020 GMT
    Subject: C=US, O=VISA, OU=Visa International Service Association,
CN=GP Root 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=Digital Signature Trust Co., OU=DST-Entrust GTI CA
    Validity
        Not Before: Dec  9 00:02:24 1998 GMT
        Not After  : Dec  9 00:32:24 2018 GMT
    Subject: C=US, O=Digital Signature Trust Co., OU=DST-Entrust GTI CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust
Co., OU=DSTCA X1,
CN=DST RootCA X1/Email=ca@digsigtrust.com
    Validity
        Not Before: Dec  1 18:18:55 1998 GMT
        Not After  : Nov 28 18:18:55 2008 GMT
    Subject: C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust
Co., OU=DSTCA X1,
CN=DST RootCA X1/Email=ca@digsigtrust.com
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network,
CN=AddTrust External CA Root
    Validity
        Not Before: May 30 10:48:38 2000 GMT
        Not After : May 30 10:48:38 2020 GMT
    Subject: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network,
CN=AddTrust External
CA Root
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VISA, OU=Visa International Service Association, CN=GP
Root 4
    Validity
        Not Before: Aug 17 00:19:00 2000 GMT
        Not After : Aug 16 23:59:00 2020 GMT
    Subject: C=US, O=VISA, OU=Visa International Service Association,
CN=GP Root 4
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=CA, ST=ON, L=Toronto, O=FortEngine Inc., OU=Certification
Authority Division, CN=fortengine/Email=ca@fortengine.com
    Validity
        Not Before: Jan 1 00:00:00 1998 GMT
        Not After : Jan 17 00:00:00 2038 GMT
    Subject: C=CA, ST=ON, L=Toronto, O=FortEngine Inc., OU=Certification
Authority Division, CN=fortengine/Email=ca@fortengine.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust
Root 4
    Validity
        Not Before: Aug 13 13:51:00 1998 GMT
        Not After : Aug 13 23:59:00 2013 GMT
    Subject: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc.,
CN=GTE CyberTrust Root 4
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=American Express Company, Inc., OU=American Express
Technologies, CN=
American Express Certificate Authority
    Validity
        Not Before: Aug 14 22:01:00 1998 GMT
        Not After : Aug 14 23:59:00 2006 GMT
    Subject: C=US, O=American Express Company, Inc., OU=American Express
Technologies, CN
=American Express Certificate Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After : Jan 7 23:59:59 2004 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Jan  7 23:59:59 2004 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS Incorp. By
Ref. Liab.LTD., OU=For VeriSign authorized testing only. No assurances (C)VS1997
    Validity
        Not Before: Mar  4 00:00:00 1997 GMT
        Not After  : Mar  4 23:59:59 2025 GMT
    Subject: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS
Incorp. By Ref. Liab. LTD., OU=For VeriSign authorized testing only. No assurances
(C)VS1997
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
    Validity
        Not Before: Dec  2 21:38:51 1999 GMT
        Not After  : Jul 10 21:38:51 2005 GMT
    Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test CA (1024 bit)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
    Validity
        Not Before: Jun 15 02:14:29 1997 GMT
        Not After  : Jul 15 02:14:29 1997 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
    Validity
        Not Before: Jun 14 22:54:45 1997 GMT
        Not After  : Jul 14 22:54:45 1997 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
    Validity
        Not Before: Apr 22 14:39:14 1997 GMT
        Not After  : Apr 22 14:39:14 1998 GMT
    Subject: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority
    Validity
        Not Before: Apr  2 17:35:53 1997 GMT
        Not After  : Apr  2 17:35:53 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority
    Validity
        Not Before: Apr  2 17:33:36 1997 GMT
        Not After  : Apr  2 17:33:36 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt
    Validity
        Not Before: Apr  2 17:35:59 1997 GMT
        Not After  : Apr  2 17:35:59 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt, CN=U
SER
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes
Only, CN=Entrust Demo Web CA
    Validity
        Not Before: Apr 26 13:35:01 1996 GMT
        Not After  : Apr 26 13:35:01 2006 GMT
    Subject: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes
Only, CN=Entrust Demo Web CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
    Validity
        Not Before: Dec  2 21:35:48 1999 GMT
        Not After  : Jul 11 21:35:48 2005 GMT
    Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=development, CN=CryptSoft Dev CA
    Validity
        Not Before: Mar 22 13:34:04 1997 GMT
        Not After  : Mar 22 13:34:04 1998 GMT
    Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=development, CN=CryptSoft Dev CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=WORTHLESS CERTIFICATION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES
ONLY
    Validity
        Not Before: Apr  3 13:22:54 1997 GMT
        Not After  : Apr  3 13:22:54 1998 GMT
    Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=WORTHLESS CERTIFICATION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES
ONLY
-----END CERTIFICATE-----

```

- **CSCdy89507**

**Symptom:** When ACNS network users use an external authentication server such as TACACS+, RADIUS, Windows NT LAN Manager (NTLM), or Lightweight Directory Access Protocol (LDAP) for authentication, authorization, and accounting of user accounts, the authentication server settings cannot be changed.

**Condition:** This occurs in ACNS software, Release 5.0 and later.

**Workaround:** Users need to remove the authentication server from service when they want to change the settings for any of the external authentication servers, such as TACACS+, RADIUS, NTLM, or LDAP. This can be done using the Local Authentication Settings window or the Authentication Scheme Settings window in the Content Distribution Manager GUI.

- CSCdz32182

Symptom: When the user tries to add port 8443 for incoming HTTPS proxy requests on a Content Engine using the **https proxy incoming 8443** EXEC command, the following message appears:

```
Port 8443 is reserved for application the Cdm_UI_http
```

Condition: This problem occurs when port 8443 is reserved for the HTTPS incoming proxy by the Content Distribution Manager GUI and port 8443 cannot be used on a Content Engine where no Content Distribution Manager GUI is running. However, on a Content Distribution Manager, it is appropriate to reserve port 8443, because this port is used as the Content Distribution Manager GUI port.

Workaround: Use a different port that is not reserved. You can check reserved ports using the **show services port *port-number*** EXEC command for a specific port or **show services summary** EXEC command for a collective summary of all used ports.

- CSCdz35191

Symptom: For pre-positioned Windows Media content, if the content is defined in the manifest file to be WMT over HTTP play and if NTLM authentication is enabled from the Content Distribution Manager, the Content Engine fails to handle the authentication with the origin server properly. You are repeatedly prompted for a username and password even though you have already entered the proper username and password.

Condition: This occurs in ACNS software, Release 5.0 and later.

Workaround: Choose one of the following workarounds:

- Use MMS play rather than HTTP play in the manifest file definition.
- Use HTTP play, but disable authentication.
- Use HTTP play with basic authentication.

- CSCdz41188

Symptom: The cache service unexpectedly restarts after running for 3 months.

Condition: The cache service automatically restarts when it runs for a relatively long time under production traffic.

Workaround: The cache service is automatically restarted by a node manager. Therefore, no special workaround action needs to be performed.

- CSCdz44596

Symptom: A multicast receiver Content Engine obtains content through unicast before the multicast sender has delivered the content through multicast.

Condition: This problem occurs when the Content Engine has a parent forwarder that is not the multicast sender, but which has already received the content. The Content Engine contacts the parent and downloads the content through unicast.

Workaround: Use one of the following workarounds:

- Configure the channel to multicast-only in the Modifying Channel window in Content Distribution Manager GUI.
- Place the receiver Content Engine directly under the multicast sender, so that the multicast sender is the forwarder for the Content Engine.

- CSCdz67216

Symptom: The CLI does not allow you to assign a device group and reports only the first Content Engine with insufficient space. You might have to try a few times to assign a device group.

Condition: You are using the CLI to assign a device group to a channel, and multiple Content Engines have insufficient space for the channel quota.

Workaround: Either verify which Content Engines have space before you use a CLI command, or make sure that device groups contain similar Content Engines and that Content Engines are assigned consistently to device groups.
- CSCdz74319

Symptom: Users receive a DNS failure message when the caching process is unable to resolve the host names presented in the URL.

Condition: DNS failure occurs when users attempt to access a website. However, this symptom is transient and rare.

Workaround: Use the reload function of the browser, although the problem vanishes on its own after a short while.
- CSCdz75101

Symptom: An error alert on the system log page indicates a failure to configure an IP address.

Condition: This problem occurs if the Content Distribution Manager accepts an invalid IP address that you have entered in the Primary Domain Server field in NTLM Server Settings for Content Engine window.

Workaround: Make sure that you enter a valid IP address.
- CSCdz86310

Symptom: When a user configures certain settings for RealProxy, RealServer, or WMT using CLI commands, the following message appears:

```
The evaluation has already expired
```

However, when the same settings are configured using the GUI, no error message is displayed, but an error is recorded in the System Message Log window in the Content Distribution Manager GUI.

Condition: This problem occurs when an evaluation license is used and the evaluation period has expired.

Workaround: Purchase and install a permanent license. Do not use the evaluation license anymore.
- CSCea14491

Symptom: If the server responds with a “100 Continue” message to a POST request from the user, the Content Engine stops parsing all requests on the connection, and subsequent requests are not handled properly.

Condition: This symptom occurs in ACNS software, Release 4.2.5 or earlier, and all 5.0.x releases.

Workaround: To partially address the problem with proxy connection, users can upgrade to ACNS software, Release 4.2.7 and later, in which the ACNS network closes the connection after serving the request. This results in slightly higher latency because of a break in the persistent connection. Known servers respond with the “100 Continue” message to the POST request method only.

- CSCea25617

Symptom: Login and configuration authentication servers can be enabled without your having to configure an IP address or host name. For example, even if no TACACS+ servers are configured, you can still enable login authentication using TACACS+. This can be verified by using the **show authentication user EXEC** command and **authentication login tacacs enable** global configuration command.

Condition: When the **no authentication configuration local** global configuration command is used to disable local authentication, the CLI believes that TACACS+ authentication has already been enabled and allows users to disable local authentication for login. In this scenario, the user can never log in to the Content Engine, because there are no configured TACACS+ servers and local authentication is also disabled.

Workaround: There is no known workaround.
- CSCea27285

Symptom: Users cannot play live streaming content from a Windows Media Server that is trying to obtain a stream from a Content Engine broadcast station alias.

Condition: This problem occurs when a Microsoft Windows Media Server is configured to obtain a WMT live stream from the Content Engine. The user's media player receives a "corrupted data" error or "invalid state" error. This problem does not occur if the stream that has been obtained from the Content Engine is not a live stream. The Windows Media Server is failing to retrieve the stream from the Content Engine, which in turn is obtaining the stream from the origin server.

Workaround: There is no known workaround. If possible, users should use a Content Engine to obtain the stream from a Windows Media Server.
- CSCea27565

Symptom: The F1 key might not work with certain terminal settings to access the BIOS menu.

Condition: This symptom only occurs on either the CE-7305 or the CE-7325 only. With certain terminals, the F1 key might not work well because the terminal emulation program might use the F1 key for its own purposes, or send an incorrect F1 key sequence to the Content Engine. Without the F1 key, the user cannot press F1 to access the BIOS menu at system boot time.

Workaround: Tune the terminal emulation program settings, or connect a keyboard and monitor to the Content Engine to access the BIOS.
- CSCea36192

Symptom: When a user enables streaming (RTSP, WMT, and Cisco Streaming Engine) on the Content Engine Network Module from the Content Distribution Manager GUI, some of the streaming configuration settings are lost. These include WMT license key installed, RTSP server real-subscriber accept-license-agreement, rtsp server real-subscriber enable, rtsp proxy media-real enable, rtsp proxy media-real license-key installed, rtsp ip-address rtsp server, and cisco-streaming-engine enable.

Condition: This symptom occurs when the user performs a software upgrade or downgrade after applying the settings.

Workaround: The user must choose the RTSP and WMT settings from the Contents pane in the Content Distribution Manager GUI and resubmit the configurations.
- CSCea43509

Symptom: The Content Distribution Manager GUI shows that an upgrade on a Content Engine has failed when the upgrade has in fact been successful. However, the CLI on the Content Engine shows the correct upgrade information.

Condition: This symptom occurs because the upgrade meta file has the wrong software version. In other words, the version in the meta file does not match the version of the upgrade file.

Workaround: There is no known workaround.

- CSCea46917

Symptom: The Windows Media Player will continue to wait forever to play a media file if the source is a media file that is configured to play in a loop from the Windows Media Server, and if the Content Engine is configured for unicast-in multicast-out multicast delivery of streaming media.

Condition: This occurs only when the source is a Windows Media Server, the media file is configured to loop, and the Content Engine is configured for unicast-in multicast-out.

Workaround: Avoid using a loop file from the Windows Media Server. Users can pre-position the media file to the Content Engine and multicast the file from the local disk before configuring it to play in a loop.

- CSCea51815

Symptom: Content Engine model CE-565 shows lower HTTP performance when attached to an SA-7 Storage Array than when it is not attached to an SA-7.

Condition: This problem occurs when the CE-565 has WMT enabled and is attached to an SA-7 Storage Array.




---

**Note** The Storage Array is used for the cache file system (cfs).

---

Workaround: Allocate less disk space to the cfs if a Storage Array is attached to the Content Engine.

- CSCea59264

Symptom: When a user submits information in the WMT Multicast Stations window to the Content Distribution Manager using the Content Distribution Manager GUI, ACNS software displays an error message.

Condition: This problem occurs when there is a leading space entered in the Address field.

Workaround: Return to the WMT Multicast Stations window and resubmit the information after entering the address without a leading space.

- CSCea60143

Symptom: Performing a software upgrade or downgrade using the Content Distribution Manager GUI shows the status as updateFailed in the device listing windows, such as the Content Engines window. This failure occurs when the software upgrade or downgrade encounters an error on the target device. Once a request for an upgrade or downgrade is received by the target device, attempts to upgrade or downgrade software occur only once.

Condition: This occurs in ACNS software, Release 5.0 and later.

Workaround: Avoid some of the following common error conditions:

- Do not manually reload the target device if the software upgrade or downgrade status is shown as Pending or in an intermediate state (such as Downloading or Writing Flash).
- Check whether there is a pending update that has already been written to flash memory using the **show flash EXEC** command. If any pending update is found, reload the device.
- In the case of a pre-positioned update file URL, ensure that the file is fully replicated on that Content Engine before triggering a software upgrade or downgrade.
- In the case of a direct update file URL, ensure that the device can successfully connect to the target host for an FTP or HTTP download and that the specified update file is present.

If any of the above errors occur, clear that error and request another software upgrade or downgrade using the Content Distribution Manager GUI.

- CSCea88122

Symptom: After thousands of playlist position changes for a playlist that is scheduled to loop playback continuously or for an extended period, the TV-out service might run out of memory. Interruption in playback occurs, and core files are generated.

Under some error conditions, such as loss or unavailability of media files on the cdnfs, a playlist might change its position rapidly, thereby exhibiting this behavior after several hours of continuously failed playback.

Condition: This occurs on the CE-507-AV, CE-560-AV, and CE-510 or CE-560 with optional AV decoder card installed, running ACNS software, Release 5.0 or later.

Workaround: Perform any of the following workarounds:

- Disable and reenable TV-out service on the Content Engine using the **no tvout enable** and **tvout enable** global configuration commands.
- Correct any error conditions that cause rapid playlist position changes.
- Schedule TV-out playback so that playlists are periodically stopped and restarted according to various repeat intervals.

- CSCea88838

Symptom: The Content Engine does not accept the DHCP address, and the Centralized Management System (CMS) is not enabled. The Content Distribution Manager therefore indicates that the device is inactive.

Condition: When autoregistration is disabled and reenabled on a Content Engine, the DHCP offer is not accepted because the Content Distribution Manager host name cannot be resolved. This occurs if there is an interface that does not have an IP address through which the Content Distribution Manager host name can be resolved.

Workaround: Do not disable and reenable autoregistration. If you reenable autoregistration, reboot the Content Engine to accept the DHCP offer, and to restart the CMS to register the Content Engine with the Content Distribution Manager.

- CSCea89557

Symptom: The **acquirer check-time-for-old-content** [**channel-id** *channel\_num* | **channel-name** *channel\_name*] EXEC command does not work. The following messages are displayed when the command is used with valid root Content Engine channel ID and names:

```
ContentEngine# acquirer check-time-for-old-content channel-id 291
Unable to get the channel information record for channel= 291
This CE is not the root CE for this channel = 291
Failed to check the last modified time in DB
```

```
ContentEngine# acquirer check-time-for-old-content channel-name channeltest
Unable to get the channel information record for channel= 291
This CE is not the root CE for this channel = 291
Failed to check the last modified time in DB
```

Workaround: Use the **acquirer check-time-for-old-content** EXEC command without the **channel ID** or **channel name** options. This command will display the incorrect last modified time for all channels of the root Content Engine.

- CSCea90203

Symptom: A socket write error occurs when users try to disable a nonexistent port channel using the **no interface PortChannel** global configuration command.

Condition: This error occurs on the Content Engine models CE-7325, CE-7305, CE-7320, and CE-510, because there is no port channel configuration on these Content Engines.

Workaround: Do not use the **no interface PortChannel** global configuration command for nonexistent port channels.

- CSCea91755

Symptom: When ACNS software is upgraded, the database upgrade fails because a database table is found to exist already. This appears as an upgrade error in the syslog.txt log file. The Centralized Management System (CMS) does not start on the device, and the device appears as offline in the device listing windows in the Content Distribution Manager GUI.

Condition: If a device is downgraded from ACNS software, Release 5.0.11 to ACNS software, Release 5.0.1, and subsequently deregistered from the Content Distribution Manager and reregistered with the Content Distribution Manager, the local database tables that were created as part of ACNS software, Release 5.0.11 remain in the database. The existence of these tables causes a later ACNS software upgrade to fail.

Workaround: This problem occurs only if the downgraded device is deregistered from the Content Distribution Manager. However, it is also possible to downgrade a device, keep it registered with the Content Distribution Manager, and later upgrade the device. In situations that require the downgraded device to be deregistered from the Content Distribution Manager, the database needs to be cleared of all tables before you reregister the device.

The sequence of CLI commands to deregister and reregister a device is as follows.

1. **cms deregister**
2. **cms database delete**
3. **cms enable**

The **cms deregister** EXEC command removes the registration information from the Content Distribution Manager and removes known database tables. The **cms database delete** command removes all tables, including any table that might have been created as part of another ACNS software release. The **cms enable** command registers the device with the Content Distribution Manager, creates the local database, and starts the CMS processes.

- CSCea93249

Symptom: Installing an upgraded version of ACNS software, Release 5.0.x deletes all content in the existing SmartFilter directory. Therefore, if SmartFilter software was previously installed for URL filtering, installation of a newer version of ACNS software, Release 5.0.x causes filtering to be disabled.

Condition: This symptom occurs if the user installs an upgraded version of ACNS software, Release 5.0.x on a Content Engine running SmartFilter software.

Workaround: SmartFilter, Version 3.1.2 is shipped with ACNS software, Release 5.0.x and contains SmartFilter software policy information stored on remote SmartFilter Administration Servers. Use the SmartFilter Administration Console to reapply the configuration settings on the Content Engine, and manually download the SmartFilter Control List. Once the Control List has been downloaded to the Content Engine, URL filtering will recommence.

- CSCeb02494
 

Symptom: A multi-bit-rate (MBR) media file, after being preloaded, returns a partial cache hit after a proxy-style request.

Condition: This problem was observed with only one MBR media file.

Workaround: There is no known workaround. The media file will be fully cached after a proxy-style request is served.
- CSCeb07223
 

Symptom: When the network experiences significant packet loss, the multicast sender may send a few bytes less than the actual file size. This causes multicast reception to fail on all receivers.

Condition: The network experiences significant multicast packet loss when a multicast session is about to end.

Workaround: In the `/local1/multicast-expert-config/` directory, make the following changes in a `pgmfx` configuration file on the multicast sender:

  - Turn off Pragmatic General Multicast (PGM) congestion control.
  - Increase the proactive forward error correction (FEC).

On the Content Distribution Manager GUI, set the value of FEC to 16.
- CSCeb28575
 

Symptom: When the user tries to copy a file from the FTP server and install the software release file on the Content Engine, using the `copy ftp install {hostname | ip-address} remotefiledir remotefilename` command, the following error message appears:

```
ruby_upgrade: cannot create lock file 'ruby_upgrade.lck' : Permission denied
```

Condition: This error occurs when the user is logged in as remote user, using TACACS+ or RADIUS as the login authentication method for device management.

Workaround: Log in as admin user and perform the upgrade.
- CSCeb34946
 

Symptom: Content Engine AV models are unable to play audio-only files.

Condition: This occurs as the Content Engine is looking to synchronize audio and video tracks, but there is no video track.

Workaround: Record the audio-only files with blank video tracks.
- CSCeb35954
 

Symptom: The `show websense-server EXEC` command shows the number of licensed users as zero.

Condition: The Websense Manager contacts the Websense server when a user enters the license key and expiry date, and tries to download the Websense database from the Websense website. If the Content Engine running the Websense server fails to download the Websense database because of network filtering errors, the `show websense-server EXEC` command shows the number of licensed users as zero.

Workaround: Configure a Content Engine that can download the Websense database as a proxy in the Websense Manager.

- CSCeb37567  
Symptom: Unicast distribution is temporarily interrupted.  
Condition: This occurs when there is no multicast sender configured at the beginning of distribution.  
Workaround: There is no known workaround.
- CSCeb48853  
Symptom: Services do not start in ACNS software, and no message is displayed.  
Condition: When a default gateway is not configured, services do not start.  
Workaround: Configure a default gateway in the ACNS software GUI.
- CSCeb56333  
Symptoms: An SNMP query to ccmHistoryEventTable on a Cisco Content Engine returns Management Information Base (MIB) instances with a fixed index. According to the definition of the CISCO-CONTENT-ENGINE-MIB, each new event stored in this table should be assigned a progressive unique index.  
Condition: This problem occurs on Cisco Content Engines running ACNS software, Release 5.0.3 or earlier.  
Workaround: There is no known workaround.
- CSCeb77349  
Symptom: When a Content Engine is configured for RADIUS authorization, the Content Engine sends two distinct Access-Requests to the authentication, authorization, and accounting (AAA) server. The second Access-Request is identical to the first, except for the RADIUS ID. This similarity causes problems with one-time-password (OTP) servers, which do not accept the second request (carrying an identical password as the first one), and send back an Access-Reject, causing the Content Engine to deny access to the user.  
Condition: The problem is observed when users try to log on to the Content Engine using Telnet.  
Workaround: There is no known workaround.
- CSCeb83282  
Symptom: When IP address changes are made on the Content Engine with WCCP enabled, existing connections break, and for 30 seconds new connections are not accepted.  
Condition: This problem occurs when users change IP addresses on the Content Engine with WCCP enabled.  
Workaround: Disable WCCP before changing IP addresses on the Content Engine.
- CSCeb85057  
Symptom: The Content Engine displays the following error message:  

```
KERNEL: assertion (atomic_read(&sk->wmem_alloc) == 0) failed
```

  
Condition: Content Engines display this error message during normal operation.  
Workaround: Ignore the error message.
- CSCec09045  
Symptom: Users do not receive the web pages they requested, or the web pages load very slowly.

Condition: This problem occurs when the Content Engine does not close an HTTP connection even after receiving a “connection:close” response from the origin server. The Content Engine keeps waiting for the server to close the connection until the connection times out, and the Content Engine does not process subsequent requests, causing delayed responses.

Workaround: Configure a static bypass entry for the origin server that causes the problem.

- CSCec21671

Symptom: The Content Engine GUI loads slowly and some images on the GUI do not load.

Condition: This problem occurs when TACACS+ is enabled as the primary authentication method for login and configuration access to the Content Engine.

Workaround: Use the local user ID with local authentication as the primary authentication method.

- CSCec31432

Symptom: The transaction log shows a cache miss for Range requests for pre-positioned content.

Condition: This problem occurs when a request for pre-positioned content contains HTTP Range request headers.

Workaround: There is no known workaround.

- CSCec36290

Symptom: Users employing a client computer running Windows XP with Windows Media Player 9.0.0.3008 cannot retrieve embedded Microsoft media files (for example, .asf files) over HTTP from a Content Engine that has the media files pre-positioned.

Condition: This problem occurs when all the following conditions exist:

- The client computer runs Windows XP with the latest patches and has Windows Media Player 9.0.0.3008 installed.
- The Content Engine has the content pre-positioned, and the content must be retrieved over HTTP because the Content Engine is not configured for WMT or a proxy.
- The media file is accessed using an embedded media player.

Workaround: Use one of the following workarounds:

- Use a client computer that runs Windows 2000.
- Use a different version of the Windows Media Player.
- Enable WMT on the Content Engine.

- CSCec70872

Symptom: Users cannot access the Content Engine using the GUI or Telnet because the root file system partition is full.

Condition: This problem occurs when users deploy rules from the SmartFilter Administration Console.

Workaround: There is no known workaround.

- CSCec78732

Symptom: Users experience long delays while using LDAP for authentication, and they see several prompts before successful authentication.

Condition: This problem occurs when users try to use LDAP for authentication.

Workaround: Try again, and the authentication will succeed.

- CSCec88324
 

Symptom: The Content Engine does not send SNMP traps when a disk is unreachable or pulled out of the device.

Condition: This problem occurs when SNMP is configured on the Content Engine, and the disk is not reachable or taken out of the device.

Workaround: There is no known workaround.
- CSCed11183
 

Symptom: Websense filtering stops working when Websense is configured to use custom filters.

Condition: This problem occurs when custom filtering is used in Websense.

Workaround: There is no known workaround.
- CSCed13700
 

Symptom: When users attempt to edit the list of locations using the Locations window in the Content Distribution Manager GUI, an error appears, indicating that the user might have clicked the Back button or Refresh button in the browser window.

Condition: This problem occurs when there are a large number of locations, and users try to edit locations before the complete list is loaded.

Workaround: Wait for the complete list of locations to be loaded before making any changes.
- CSCed62969
 

Symptom: The cms\_cdm service in the Content Distribution Manager restarts, causing the Content Distribution Manager GUI to stop responding for a short time. The cms\_cdm\_start\_log in the Content Distribution Manager shows the following errors:

```
Tue Feb 03 07:53:45 GMT-06:00 2004 [E] FileManager: java.lang.NullPointerException:
java.lang.NullPointerException
    at
com.cisco.unicorn.controller.FileManager.checkIfModified(FileManager.java:209)
    at com.cisco.unicorn.controller.FileManager.runImpl(FileManager.java:155)
    at com.cisco.unicorn.server.AModule.run(AModule.java:177)
    at java.lang.Thread.run(Thread.java:484)
```

Condition: This problem occurs very rarely.

Workaround: There is no known workaround. The cms\_cdm service automatically restarts, and causes only a temporary disruption in the Content Distribution Manager GUI.
- CSCin14344
 

Symptom: No CLI command is available in ACNS software, Release 5.0 and later releases to clear WCCP generic routing encapsulation (GRE) packet-related information. Although a CLI command (**show wccp gre**) is available to display the WCCP GRE counters, there is no CLI command currently available to clear them.

Condition: This symptom is observed regardless of whether WCCP is enabled or disabled on the Content Engine.

Workaround: There is no known workaround.

- CSCin19219

Symptom: Any changes in the Content Engine's DNS cache configuration do not take effect immediately.

Condition: This situation occurs when the **dns listen** and **dns pin** global configuration commands are used to configure an IP address and port number to listen for requests and map the IP addresses to their corresponding host names.

Workaround: Use the **no dns enable** and **dns enable** commands to disable and enable the Content Engine's DNS caching server, which causes the DNS caching server pick up the changed configurations.

- CSCin28274

Symptom: Under certain conditions, if the user configures one valid and one invalid FTP server for exporting transaction logs, the **show statistics transaction-logs EXEC** command displays the entry for the valid FTP server twice. As a result of the duplicate entry, the counters are not correspondingly incremented with the number of files that are exported through FTP.

Condition: This symptom is observed on Content Engines running ACNS software, Release 5.0.

Workaround: Use the **clear statistics transaction-logs EXEC** command to clear the transaction log export statistics and the duplicate entry for the valid FTP server.

- CSCin30153

Symptom: The client does not receive a requested object if the Websense server is not reachable or if the Websense server timeout value is greater than the configured default timeout value.

Condition: This symptom is observed only under the following conditions:

- The request from the client is a transparent request.
- URL filtering through Websense is enabled in the Content Engine.
- The Websense server is not reachable.
- The Websense server timeout value is greater than 60 seconds.

Workaround: Configure a Websense server timeout value must be configured to be less than 60 seconds.

- CSCin35914

Symptom: The Software Update File Registration window in the Content Distribution Manager GUI displays the following error message for a valid meta file URL:

```
Transaction not completed
sun.net.ftp.FtpProtocolException:port
```

Condition: This occurs when the Content Distribution Manager host name contains numeric values. For example, if the software update file URL is 7305.cisco.com, Linux systems encounter problems when Java attempts to resolve the URL to an IP address. This is because only 7305 is considered instead of 7305.cisco.com. As a result, the URL is resolved to a strange IP address, 0.0.28.137 for 7305, causing the Content Distribution Manager GUI to display an error message even though the meta file URL might be valid. This problem also occurs if the update meta file is hosted on an FTP server.

Workaround: Perform one of the following workarounds:

- Make sure that the Content Distribution Manager host name contains at least one nonnumeric value.
- Host the update meta file on an HTTP server and use the HTTP URL instead of an FTP URL for performing software updates.

- CSCin41994
 

Symptom: If the **cdnfs browse** EXEC command is used and the filename or the directory name of pre-positioned content contains a space, the command does not display the information contained in the file, nor does it browse through the cdnfs files and directories.

Condition: This occurs in Content Engines running ACNS software, Release 5.0.11.

Workaround: There is no known workaround.
- CSCin42531
 

Symptom: When there are more than 10 bandwidth records in the Bandwidth Setting for Device Groups window and the user tries to navigate to any other window using the pagination counter at the bottom of the window, an error message is displayed.

Workaround: Choose All or a number higher than the default value (10) in the Rows field to display the record you want to edit.
- CSCin55484
 

Symptom: A pre-positioned content object is lost after you configure the disk and reload the Content Engine.

Condition: If the amount of cdnfs content present is close to the amount of disk space allocated to the cdnfs, then cdnfs content is removed to ensure that the cdnfs file system can be resized properly to hold the saved content. In ACNS software, Release 5.0.x, when you perform a disk configuration, the content is moved out of the file system (if other file systems that can hold the content are detected) or deleted (if other file systems that can hold the content are not detected) when you perform a disk configuration, if 90 percent or more of the cdnfs file system is used.

Workaround: Use one of the following workarounds:

  - Do not perform disk configuration.
  - Ensure that the amount of content present is less than 90 percent of the disk space allocated to the newly specified cdnfs file system.
  - Upgrade to ACNS software, Release 5.1, which always preserves content when you perform a disk configuration, regardless of the amount of disk space specified for the cdnfs.

## Resolved Caveats - ACNS Software, Release 5.0.11

- CSCeb49014
 

In ACNS software, Release 5.0.3, if a channel is using a crawl job to acquire contents, all content is deleted when a new root Content Engine is chosen or the old root Content Engine goes offline and a temporary root Content Engine is chosen.
- CSCeb50137
 

If *cdn-url* attribute is used for live content and *src* attribute is changed in the manifest file after the live content is acquired, the acquirer in ACNS software encounters an infinite loop and stops performing acquisition tasks. The acquirer in ACNS software also creates internal cdnfs files constantly until the Content Engine reaches its allotted limit of cdnfs files. The Content Engine then reports following errors in the syslog file:

```
sumf.c: hit limit of number of UNS-UFM table entries (2097152)
In acquirer error log: /local1/errorlog/acquirer-errorlog.current
01/16/2004 07:52:34.192(Local)(10051)ERRO:ADUns.cpp:48-> 240, Uns return error in:
uns_obj_create(url=http-localhost-C9IMNioFkwzI3pGaapS8aA/broadcast1-cisco-ad-temp-1074
261153,size=0), error=31 (Too many CDN files (cannot add to UFM))
```

The **show acquirer progress** EXEC command does not return any output.

- CSCec34608

Microsoft Internet Explorer closes if there is no home page specified in the browser settings, and the first request for content from the browser is an HTTPS request. This problem occurs under the following conditions:

- The client computer uses Microsoft Internet Explorer browser version 6.0.2600.0000.xpclnt\_qfe.021108-2107CO running on Windows XP.
- The Content Engine is set up as a proxy server.
- LDAP authentication is enabled on the Content Engine.

- CSCec42245

The Content Distribution Manager GUI forces users to specify an outgoing proxy when users check the **Preserve 407 headers** check box in the HTTP Connection Settings window.

- CSCec55785

The downgrade process fails on a Content Engine 7320 when users try to downgrade from ACNS software, Release 5.0.x to ACNS software, Release 4.2.

- CSCed02248

After users reboot the Content Engine, ACNS software fails to apply WMT broadcast alias-name configurations from the running configuration on startup.

- CSCed23995

Content Engines generate syslog messages indicating that E-CDN files are missing for some URLs. This problem occurs when all the following conditions exist:

- The Content Engine contains E-CDN files, which were created when the Content Engine was running ACNS software, Release 4.x or E-CDN Software, Release 3.x.
- The Content Engine contains multiple disk drives, which may include Storage Array devices.
- Some of the disk drives have been replaced.
- The replaced disk drives contain E-CDN files.
- The disk drives, that were not replaced, have cdnfs space assigned, and have cdnfs entries.

- CSCed28289

The Content Engine blocks non-HTTP requests from clients.

- CSCed29450


The node manager in ACNS software does not remove the start\_log files from the /local/local1/service\_logs/ directory if there are a large number of start\_log files in this directory when the Content Engine boots up.

- CSCed40688

The Content Engine serves the wrong web page when WCCP intercepts a client request with an incorrect IP address for the web server. The Content Engine caches the wrong web page and serves the cached page if multiple clients request the same page (with the incorrect IP address of the web server in the request).

- CSCed44017

The Content Engine stops responding to HTTP requests when the HTTP DNS cache fails to send DNS queries on a DNS cache miss.

- CSCed45228  
When a Content Engine running ACNS software, Release 5.1.x is downgraded to ACNS software, Release 5.0.x, the HTTP caching process continually stops, and the node manager keeps restarting the HTTP caching process.
  - CSCed46596  
The Content Distribution Manager GUI and the **show statistics replication** EXEC command output on the root Content Engine shows the replication status as “crawling and acquiring” even after the crawl job for the channel has been completed. The **show statistics acquirer job-list** EXEC command output show that the crawl job has been completed for the channel.
  - CSCed47553  
The ACNS network file system (cdnfs) stores pre-positioned ACNS network content that is to be delivered by all of the supported protocols, including HTTP, WMT, MMS, and RTSP. The **cdnfs cleanup** EXEC command, which can be used to clean up unused unified name space (UNS) content, does not work properly in the following situations:
    - When an ACNS software bug is encountered, a temporary unified name space (UNS) object is created on the device. The **cdnfs cleanup** command does not remove these temporary, unused UNS objects.
    - For each pre-positioned file, ACNS software creates two UNS objects on the device: a CDN UNS object for storing attributes, and a resource UNS object for storing the actual data file. The **cdnfs cleanup** command removes all of the CDN UNS objects, which prevents the root Content Engine from serving all pre-positioned files.
- 
- 

**Note** The **acquisition-distribution database-cleanup** command (which should detect whether the CDN UNS object or the resource UNS object is missing, and if so, notify the ACNS software to pre-position them again) fails to do so.
- 
- CSCed47571  
For each pre-positioned file, ACNS software creates two UNS objects on the device: a CDN UNS object for storing attributes, and a resource UNS object for storing the actual data file. ACNS software fails to restore the CDN UNS objects if the **cdnfs cleanup** EXEC command, which is used to clean up unused unified name space (UNS) content, removes valid CDN UNS objects.
  - CSCed50633  
The Content Router displays the message “Preload did not receive overload message. Preload may not be running”, when the Content Router is overloaded.
  - CSCed53548  
The mms\_server process on the Content Engine generates core files and restarts.
  - CSCed56746  
If the manifest file has not been changed for a long time, ACNS software does not recheck the contents and redo all crawl jobs in the channel when users click the **Fetch Manifest** button in the Modifying Channel window in the Content Distribution Manager GUI.
  - CSCed57179  
While replicating content for a channel through multicast distribution, the receiver Content Engine does not save the new version of a pre-positioned content file, but retains and serves the old version when clients request the file.

- CSCed57751  
The caching process on Content Engines generates core files and restarts on Content Engines when the SmartFilter plug-in is enabled and there is a high load on disk memory.
- CSCed59522  
If a file that has been distributed through multicast is overwritten on the origin server with a file having the same filename but an older time stamp, the acquirer in ACNS software acquires the file again, but the multicast sender Content Engine does not send the file again to multicast receivers.
- CSCed60070  
In Content Engines running ACNS software, Release 5.0.x, the snmpcd process stops responding when the hrStorageTable is queried for the following MIB object instances:
  - hrStorageIndex.0
  - hrStorageType.0
  - hrStorageDescr.0
  - hrStorageAllocationUnits.0
  - hrStorageSize.0
  - hrStorageUsed.0
  - hrStorageAllocationFailures.0
- CSCed63026  
The sfagent process on a Content Engine (running ACNS software, Release 5.0.9 or later with SmartFilter URL filtering enabled) generates core files and restarts.
- CSCed63881  
The Content Engine receives a “401 Unauthorized” error while acquiring content over Secure Socket Layer (SSL). The acquirer log files in the Content Engine indicate that the security certificate has expired or the issuer of the certificate is not recognized, although the certificates have been issued by a standard certificate authority (CA).
  - The acquirer log file shows “Certificate expired” errors if the website has a certificate issued with any one of the following issuer details:
 

```
C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority
C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority
C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
O=European ICE-TEL project, OU=V3-Certification Authority, L=Darmstadt
O=European ICE-TEL project, OU=V3-Certification Authority
O=European ICE-TEL project, OU=V3-Certification Authority, L=Darmstadt, CN=USER
C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes Only, CN=Entrust
Demo Web CA
C=US, O=RSA Data Security, Inc., OU=Commercial Certification Authority
C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd, OU=development, CN=CryptSoft
Dev CA
C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd, OU=WORTHLESS CERTIFICATION
AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES ONLY
```

- The acquirer log file shows “Issuer is not recognized” errors if the website does not have a certificate with any one of the following issuer details:

```

Subject: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority
Subject: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority
Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority
Subject: C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority
Subject: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS Incorpor. By Ref.
Liab. LTD., OU=For VeriSign authorized testing only. No assurances (C)VS1997
Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test CA (1024 bit)
Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=CA
Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
Subject: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
Subject: O=European ICE-TEL project, OU=V3-Certification Authority, L=Darmstadt
Subject: O=European ICE-TEL project, OU=V3-Certification Authority
Subject: O=European ICE-TEL project, OU=V3-Certification Authority, L=Darmstadt,
CN=USER
Subject: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes Only,
CN=Entrust Demo Web CA
Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
Subject: C=US, O=RSA Data Security, Inc., OU=Commercial Certification Authority
Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Server
CA/Email=server-certs@thawte.com
Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Premium Server
CA/Email=premium-server@thawte.com
Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd, OU=development,
CN=CryptSoft Dev CA
Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd, OU=WORTHLESS
CERTIFICATION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES ONLY

```

- CSCed65106

The Content Engine does not serve pre-positioned HTTP content when IP spoofing is turned on.

- CSCed70553

The root Content Engine displays an “Exceed Disk Quota” error, though the total file size in the channel is less than the assigned disk quota.

- CSCed73944

The Content Distribution Manager GUI displays “Internal Server Error” messages while processing replication status data. The Content Distribution Manager APIs become unavailable and the syslog files on all the Content Engines in the ACNS network display remote procedure call (RPC) errors while trying to contact the Content Distribution Manager.

- CSCed76787

When the database index file in the Content Engine is corrupted (because of failure of the hard disk), the syslog files in the Content Engine display critical error messages such as “foreign key referential integrity failure” and “RPC to replicator failed.” The **show distribution process EXEC** command returns the message “Metadata Receiver is not running.”

- CSCin59272

In HTTPS acquisition with directory indexing crawling, when the forward slash (/) is missing at the end of the starting URL, the acquirer in ACNS software fails and displays a 700 error message.

# Related Documentation

Your product shipped with a minimal set of printed documentation. The printed documentation provides enough information for you to install and initially configure your product. Refer to the *Documentation Guide* for a complete documentation roadmap and URL documentation links for this product.

## Product Documentation Set

In addition to these release notes, the product documentation set includes:

- *Documentation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

## Hardware Documentation

- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Installing the Cisco Content Engine 7305 and 7325*
- *Installing Field-Replaceable Units in the Cisco Content Engine 7305 and 7325*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Installing the Cisco Content Engine 510 and 565*
- *Installing Field-Replaceable Units in the Cisco Content Engine 510 and 565*
- *Cisco Storage Array Installation and Configuration Guide*
- *Release Notes for Cisco Content Delivery Manager 4630*
- *Cisco Content Distribution Manager 4650 Product Description Note*
- *Cisco Content Distribution Manger 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Release Notes for the Cisco Content Engine 500 Series*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

## Software Documentation

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.0*
- *Cisco ACNS Software Caching Configuration Guide, Release 5.0*
- *Cisco ACNS Software Command Reference, Release 5.0*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *Cisco ACNS Software Migration Guide, Release 5.0*
- *Cisco ACNS Software API Guide, Release 5.0*
- *Release Notes for Cisco ACNS Software, Release 5.0*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.1*
- *Creating Manifest Files for Cisco ACNS Software, Release 5.0.3*
- *Release Notes for Cisco ACNS Software, Release 5.0.3*
- *Release Notes for Cisco ACNS Software, Release 5.0.5*

- *Release Notes for Cisco ACNS Software, Release 5.0.7*
- *Release Notes for Cisco ACNS Software, Release 5.0.9*

#### Online Help

Content Distribution Manager GUI online help system

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit e-mail comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
 Attn: Customer Document Ordering  
 170 West Tasman Drive  
 San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

### Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

### Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:  
<http://www.cisco.com/go/marketplace/>
- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:  
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0402R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.