



Locking Your Door in BMC CONTROL-M/Enterprise Manager

Kim Delgado
System Tool Support
Hewitt Associates

Agenda



- › About Hewitt Associates
- › Hewitt's Reasons for Locking Down the Environment
- › Software Requirements
- › Generating a Certificate for BMC[®] CONTROL-M/Server, BMC[®] CONTROL-M/Enterprise Manager Mainframe Gateway and BMC[®] CONTROL-M/Agent
- › Hints and Tricks

About Hewitt Associates



- › A global management consulting and employee benefit delivery firm
- › The world's largest provider of multi-service HR business process outsourcing
- › Approximately 22,000 associates and offices in 35 countries spanning the globe

Hewitt's Requirements for Locking Down the Environment

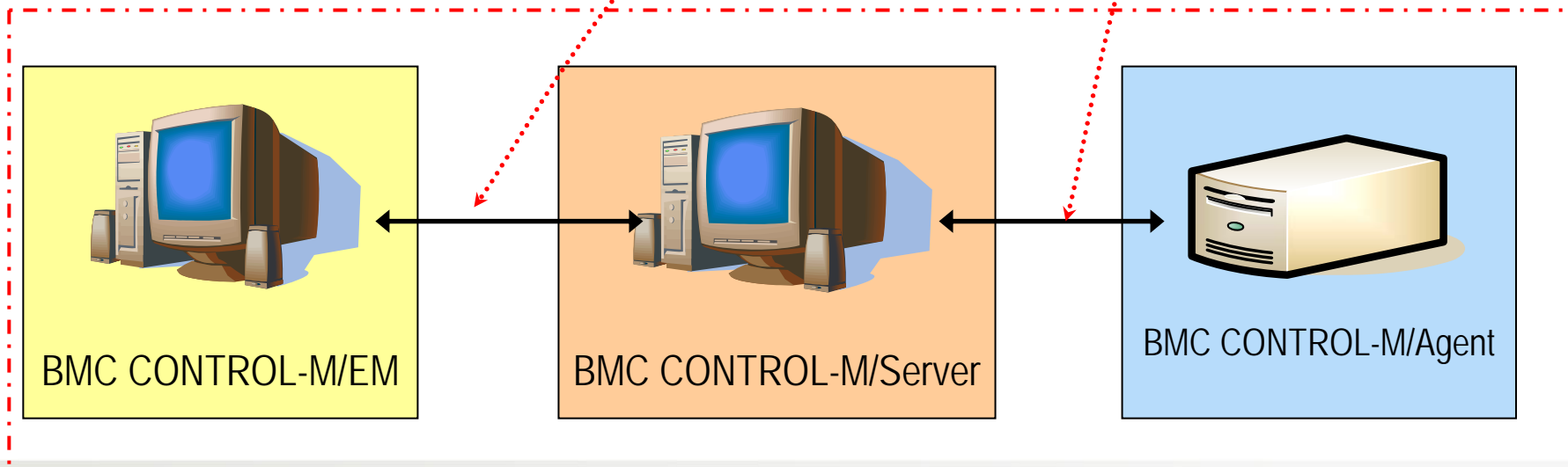


- › Lock down the BMC CONTROL-M/Enterprise Manager (BMC CONTROL-M/EM) software
 - Specified by both external and internal Hewitt clients to lockdown software
 - Sarbanes-Oxley compliant
 - Required by Hewitt's Security Department
 - **Please note:** BMC CONTROL-M/EM is delivered with default keys and certificates that are not unique. BMC Software recommends that you change these keys and certificates.

What are we trying to achieve ?



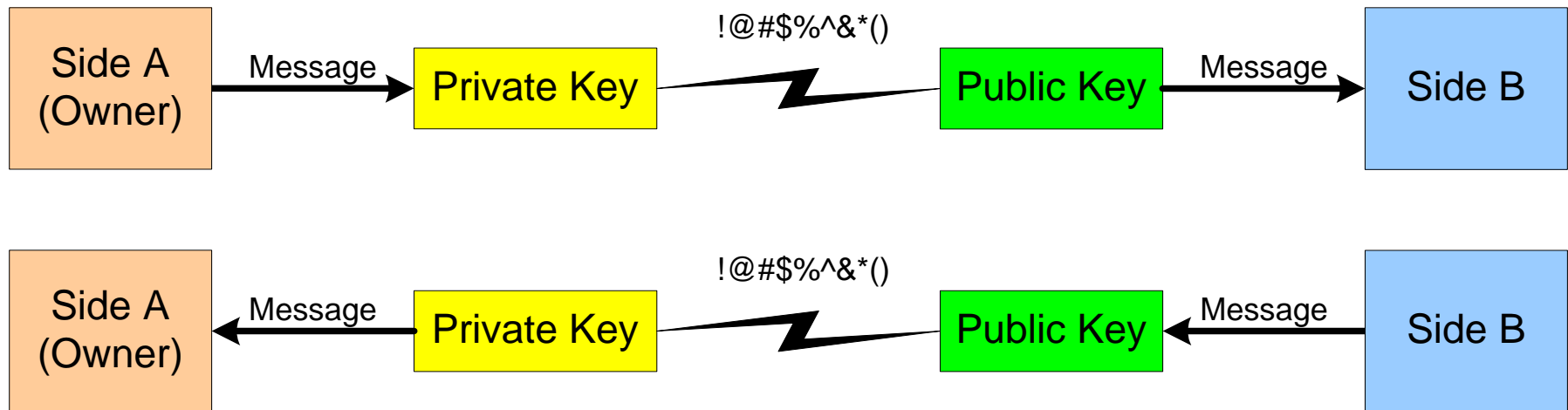
- › “bad guys” can impersonate a BMC CONTROL-M component
- › By default, communication channels are not secured
 - BMC CONTROL-M/EM to BMC CONTROL-M/Server and vice versa
 - BMC CONTROL-M/Server to BMC CONTROL-M/Agent and vice versa
- › By using SSL, these channels can be secured



How does SSL (Secured Socket Layer) Work?



- › Establishing a communication channel between two parties
 - The Public key is made public by distributing it widely
 - The Private key is never distributed; it is always kept secret
 - The communication channel is encrypted prior physically transmitting it over the network and then – decrypted once arriving its destination and assuming the keys match





- › To use Secured Socket Layer (SSL) with BMC CONTROL-M/Server, BMC CONTROL-M/Agent and BMC CONTROL-M/EM Gateway, the following components must be installed:
 - BMC CONTROL-M/EM v6.1.02 fix pack 4 and above
 - BMC CONTROL-M/Server v6.1.01 fix pack 4 and above
 - BMC CONTROL-M/Agent v6.1.01 fix pack 4 and above

Note: All BMC CONTROL-M components are provided using a default “kdb” (Key DataBase file). In order to secure your environment it is highly recommended to replace it with your own generated files. The samples presented in this session include the default KDB file that should be replaced in a “real-life” scenario.

Generating a Certificate for BMC CONTROL-M/Server



› Log into BMC CONTROL-M/Server

- Navigate to the SSL directory (cd /ctm/data/SSL/cert)
- Type: **sslcmd -k ctmkey.kdb <generated password>**
 - › 1. Generate key
 - › 2. Add CA
 - › 3. Generate CSR
 - › 4. Add cert
 - › 5. List keys
 - › 6. Delete key
 - › 7. List certs
 - › 8. List CA
 - › 9. View CA
 - › 10. Delete CA
 - › 11. Add CRL
 - › 12. Change KDB Password
 - › 13. Add Labeled Password
 - › 14. List Labeled Password
 - › 15. Delete Labeled Password
 - › 16. Import Key Pair
 - › 17. Export Key Pair
 - › 18. Change Label of Key Pair
 - › 19. EXIT
 - › Enter a choice [1 - 19]:

Generating a Certificate for BMC CONTROL-M/Server (continued)



- For BMC CONTROL-M/Server, you need two certificates generated: CODN and NSDN. Finish steps below for CODN, then go back and complete the same steps for NSDN.
 - Choose Menu: **Option 1** (Generate a Key)
 - This is where you would type your server-specific name: **CODN_testabc**
 - RSA/DSA: **RSA**
 - Key length: **1024**
 - Choose Menu: **Option 3** (Generate a CSR)
 - Output file: **/tmp/testabc_codn.csr**
 - Alias name: (same as identity above): **CODN_testabc**
 - Country: **US**
 - State: **Illinois**
 - Name: **Company Name (or other identifier you decide)**
 - Unit: **(Another identifier you decide)**
 - Common Name: **CODN_testabc**
 - E-mail address: **ctmagent@testabc.xxxxxx.com**

Generating a Certificate for BMC CONTROL-M/EM Gateway



- › Log into BMC CONTROL-M/EM Gateway
 - Navigate to the SSL directory (`cd /site/resource/ssl/cert`)
 - Type: `sslcmd -k gtwkey.kdb <generated password>`
 - » 1. Generate key
 - » 2. Add CA
 - » 3. Generate CSR
 - » 4. Add cert
 - » 5. List keys
 - » 6. Delete key
 - » 7. List certs
 - » 8. List CA
 - » 9. View CA
 - » 10. Delete CA
 - » 11. Add CRL
 - » 12. Change KDB Password
 - » 13. Add Labeled Password
 - » 14. List Labeled Password
 - » 15. Delete Labeled Password
 - » 16. Import Key Pair
 - » 17. Export Key Pair
 - » 18. Change Label of Key Pair
 - » 19. EXIT
 - » Enter a choice [1 - 19]:

Generating a Certificate for BMC CONTROL-M/EM Gateway (continued)



- BMC CONTROL-M/EM Gateway uses CODN also. Please note: You need to make sure you generate a different name for the CODN generated on BMC CONTROL-M/EM Gateway from the CODN generated on the BMC CONTROL-M/Server.
 - Choose Menu: **Option 1** (Generate a Key)
 - This is where you would type your server-specific name: **CODN_testabc**
 - RSA/DSA: **RSA**
 - Key length: **1024**
 - Choose Menu: **Option 3** (Generate a CSR)
 - Output file: **/tmp/testabc_codn.csr**
 - Alias name: (same as identity above): **CODN_testabc**
 - Country: **US**
 - State: **Illinois**
 - Name: **Company Name (or other identifier you decide)**
 - Unit: **(Another identifier you decide)**
 - Common Name: **CODN_testabc**
 - E-mail address: **ctmagent@testabc.xxxxxx.com**

Generating a Certificate for BMC CONTROL-M/Agent



› Log into BMC CONTROL-M/Agent

- Navigate to the SSL directory (`cd /ctm/data/SSL/cert`)
- Type: `sslcmd -k agkey.kdb <generated password>`
 - › 1. Generate key
 - › 2. Add CA
 - › 3. Generate CSR
 - › 4. Add cert
 - › 5. List keys
 - › 6. Delete key
 - › 7. List certs
 - › 8. List CA
 - › 9. View CA
 - › 10. Delete CA
 - › 11. Add CRL
 - › 12. Change KDB Password
 - › 13. Add Labeled Password
 - › 14. List Labeled Password
 - › 15. Delete Labeled Password
 - › 16. Import Key Pair
 - › 17. Export Key Pair
 - › 18. Change Label of Key Pair
 - › 19. EXIT
 - › Enter a choice [1 - 19]:

Generating a Certificate for BMC CONTROL-M/Agent (continued)



- Choose Menu: **Option 1** (Generate a Key)
- This is where you would type your server-specific name: **AGDN_testabc**
- RSA/DSA: **RSA**
- Key length: **1024**
- Choose Menu: **Option 3** (Generate a CSR)
- Output file: **/tmp/testabc_agdn.csr**
- Alias name: (same as identity above): **ADGN_testabc**
- Country: **US**
- State: **Illinois**
- Name: **Company Name** (or other identifier you decide)
- Unit: **(Another identifier you decide)**
- Common Name: **AGDN_testabc**
- E-mail address: **ctmagent@testabc.xxxxxx.com**

Generating a Certificate for BMC CONTROL-M/Agent (continued)



- › Send the generated csr to the department that generates your certificates.
 - We used `testabc_agdn.csr` in the previous example.
 - You can find your `testabc_agdn.csr` in the output file defined when your csr was generated (`/tmp/testabc_agdn.csr`).
 - Hewitt uses SecureFX to move the csr from the UNIX server to our desktop so that it can be attached to e-mail.



- A good source to follow along with while setting up Secured Sockets Layers (SSL), is the SSL for BMC CONTROL-M – Administrator Guide.
- Always restart BMC CONTROL-M/EM, BMC CONTROL-M/Server and BMC CONTROL-M/ Agent for changes to the key database to take affect.

Requesting Certificates to be Generated



- › Send an e-mail to the department that generates your company's certificates.
 - The csrs need to be created in a X.509 PEM format.
- › Once you receive a reply e-mail with the *.pem files, detach them to the appropriate servers.

Adding the .pem Files to BMC CONTROL-M/Server



Once you receive the generated certificates (.pem files), place them in BMC CONTROL-M/EM Gateway (/site/resource/ssl/cert) directory:

» You will also need to add your private key on each server.

- » -rw-r--r-- 1 ctmserv controlm 1034 Sep 1 2004 **ABC-CA.pem**
- » -rw-r--r-- 1 ctmserv controlm 4824 Dec 25 2005 ackey.kdb
- » -rw-r--r-- 1 ctmserv controlm 6488 Jan 12 2006 ctmkey.kdb.orig
- » --rw-r--r-- 1 ctmserv controlm 11648 Jan 25 2006 ctmkey.kdb.bk
- » -rw-r--r-- 1 ctmserv controlm 13248 Jan 25 2006 ctmkey.kdb
- » -rw-r--r-- 1 ctmserv controlm 157 Jan 25 2006 access
- » -rw-r--r-- 1 ctmserv controlm 1402 Jan 31 2006 **CODN_testabc.pem**
- » -rw-r--r-- 1 ctmserv controlm 1402 Jan 31 2006 **NSDN_testabc.pem**
- » -rw-r--r-- 1 ctmserv controlm 159 Feb 24 15:35 ac.plc
- » -rw-r--r-- 1 ctmserv controlm 809 Feb 26 05:33 site.plc
- » -rw-r--r-- 1 ctmserv controlm 159 Feb 26 05:33 ns.plc
- » -rw-r--r-- 1 ctmserv controlm 142 Feb 26 05:33 co.plc

Adding the .pem Files to BMC CONTROL-M/Server (continued)



- Once the .pem files have been added to the /ctm/data/SSL/cert directory,
 - Type: `sslcmd -k ctmkey.kdb <abcd1234>`
 - Copy generated certificate and ABC-CA.pem file to the server.
 - Select choice: **2. Add CA** – this is where you add the generic private key (ABC_CA.pem).
 - Select choice: **4. Add cert** – this is where you add CODN_testabc and NSDN_testabc.
 - » 1. Generate key
 - » 2. Add CA
 - » 3. Generate CSR`
 - » 4. Add cert
 - » 5. List keys
 - » 6. Delete key
 - » 7. List certs
 - » 8. List CA
 - » 9. View CA
 - » 10. Delete CA
 - » 11. Add CRL
 - » 12. Change KDB Password
 - » 13. Add Labeled Password
 - » 14. List Labeled Password
 - » 15. Delete Labeled Password
 - » 16. Import Key Pair
 - » 17. Export Key Pair
 - » 18. Change Label of Key Pair
 - » 19. EXIT
 - » Enter a choice [1 - 19]:

–

BMC CONTROL-M/Server Example of Verifying Certificate Information



1. Generate key
 2. Add CA
 3. Generate CSR
 4. Add cert
 5. **List keys**
 6. Delete key
 7. List certs
 8. List CA
 9. View CA
 10. Delete CA
 11. Add CRL
 12. Change KDB Password
 13. Add Labeled Password
 14. List Labeled Password
 15. Delete Labeled Password
 16. Import Key Pair
 17. Export Key Pair
 18. Change Label of Key Pair
 19. EXIT
- Enter a choice [1 - 19]:5

- > ***Label 0:
- > CODN_testabc
- > ***Label 1:
- > NSDN_testabc
- > Command successful: List keys

- > Enter to proceed

1. Generate key
 2. Add CA
 3. Generate CSR
 4. Add cert
 5. List keys
 6. Delete key
 7. **List certs**
 8. List CA
 9. View CA
 10. Delete CA
 11. Add CRL
 12. Change KDB Password
 13. Add Labeled Password
 14. List Labeled Password
 15. Delete Labeled Password
 16. Import Key Pair
 17. Export Key Pair
 18. Change Label of Key Pair
 19. EXIT
- Enter a choice [1 - 19]:7

***Label 0:
CODN_testabc
chain at 1a222
ADDITIONAL IDENTIFIER
INFORMATION
RSA public key length: 1024
bits
Valid Begin: Wed Sep 1
10:54:48 2004
Valid End: Sat Aug 29
10:54:48 2037

1. Generate key
 2. Add CA
 3. Generate CSR
 4. Add cert
 5. List keys
 6. Delete key
 7. List certs
 8. List CA
 9. **View CA**
 10. Delete CA
 11. Add CRL
 12. Change KDB Password
 13. Add Labeled Password
 14. List Labeled Password
 15. Delete Labeled Password
 16. Import Key Pair
 17. Export Key Pair
 18. Change Label of Key Pair
 19. EXIT
- Enter a choice [1 - 19]:9

***Label 0:
ADDITIONAL IDENTIFIER
INFORMATION
SIMILAR TO CERTIFICATE
INFORMATION
SHOULD SHOW THAT IT WAS
SUCCESSFULLY ADDED

Update Identities on BMC CONTROL-M/Server



- Under `/ctm/data/SSL/cert` directory, update identities --
 - `testabc-ctmserv [9] vi ns.plc`
 - `[server]`
 - **identity=NSDN_testabc**
 - `logfile=nssrv.log`
 - `security_level=3`

 - `[client]`
 - **identity=NSDN_testabc**
 - `logfile=nscln.log`
 - `keyfile=/apps/ctmserv/current/ctm/data/SSL/cert/ctmkey.kdb`
 - `testabc-ctmserv [10] cat co.plc`
 - `[server]`
 - **identity=CODN_testabc**
 - `logfile=cosrv.log`

 - `[client]`
 - `logfile=cocln.log`
 - **identity=CODN_testabc**
 - `keyfile=/apps/ctmserv/current/ctm/data/SSL/cert/ctmkey.kdb`
 - `testabc-ctmserv [11]`

Adding the .pem Files to BMC CONTROL-M/EM Gateway



Once you receive the generated certificates (.pem files), place them in
BMC CONTROL-M/EM Gateway /site/resource/ssl/cert directory:

» You will also need to add your private key on each server.

```
» -rw-r--r-- 1 ecs dba 1034 Sep 1 2004 ABC-CA.pem
» -rw----- 1 ecs dba 248 Jan 10 2006 site.plc
» -rw----- 1 ecs dba 204 Jan 10 2006 em.plc
» -rw----- 1 ecs dba 4328 Jan 12 2006 gtwkey.kdb.orig
» -rw-r--r-- 1 ecs dba 1394 Jan 13 2006 123ABC.pem
» -rw-r--r-- 1 ecs dba 6648 Jan 25 2006 gtwkey.kdb.bk
» -rw-r--r-- 1 ecs dba 8232 Jan 25 2006 gtwkey.kdb
» -rw----- 1 ecs dba 250 Jan 31 2006 gtw.plc
» -rw----- 1 ecs dba 240 Jan 31 2006 gtw.plc.bkp
» -rw-r--r-- 1 ecs dba 1394 Jan 31 2006 CODN_testabc.pem
```

Adding the .pem Files to BMC CONTROL-M/EM Gateway (continued)



- Once the .pem files have been added to the /ctm/data/SSL/cert file,
 - Type: `sslcmd -k gtwkey.kdb <abcd1234>`
 - Copy generated certificate and ABC-CA.pem file to the server.
 - Select choice: **2. Add CA** – this is where you add the generic private key (**ABC_CA.pem**).
 - Select choice: **4. Add cert** – this is where you add **CODN_testabc**.
 - » 1. Generate key
 - » 2. Add CA
 - » 3. Generate CSR`
 - » 4. Add cert
 - » 5. List keys
 - » 6. Delete key
 - » 7. List certs
 - » 8. List CA
 - » 9. View CA
 - » 10. Delete CA
 - » 11. Add CRL
 - » 12. Change KDB Password
 - » 13. Add Labeled Password
 - » 14. List Labeled Password
 - » 15. Delete Labeled Password
 - » 16. Import Key Pair
 - » 17. Export Key Pair
 - » 18. Change Label of Key Pair
 - » 19. EXIT
 - » Enter a choice [1 - 19]:

–

Update Identity on BMC CONTROL-M/EM Gateway



- %cert> vi gtw.plc
- [client]
- logfile=gtw_ssl.log
- **identity=CODN_testabc**
- keyfile=/apps/ecs/current/site/resource/ssl/cert/gtwkey.kdb
- security_level=4
- loglevel=ERROR
- password=axxxx8x7xxxxxxx,/apps/ecs/current/site/resource/local/tree.bin

Adding the .pem Files to the BMC CONTROL-M/Agent



Once you receive the generated certificates (.pem files), place them in BMC CONTROL-M/EM Gateway /site/resource/ssl/cert directory:

- » You will also need to add your private key on each server.

- » -rwxr-xr-x 1 testabc controlm 4236 Jul 26 2001 agtkey.kdb
- » -rwxr-xr-x 1 testabc controlm 5498 Apr 28 2003 tree.bin
- » -rwxr-xr-x 1 testabc controlm 42 Apr 28 2003 access
- » --rw-r--r-- 1 testabc controlm 1034 Sep 1 2004 **ABC-CA.pem**
- » -rw-r--r-- 1 testabc controlm 943 Jan 12 2006 site.plc
- » -rw-r----- 1 testabc controlm 8248 Jan 25 2006 agkey.kdb
- » -rw-r----- 1 testabc controlm 1379 Jan 31 2006 **AGDN_testabc.pem**
- » -rw-r--r-- 1 testabc controlm 182 Jan 31 2006 ag.plc

Adding the .pem Files to BMC CONTROL-M/Agent (continued)



- Once the .pem files have been added to the /ctm/data/SSL/cert file,
 - Type: `sslcmd -k gtwkey.kdb <abcd1234>`
 - Copy generated certificate and ABC-CA.pem file to the server.
 - Select choice: **2. Add CA** – this is where you add the generic private key (**ABC_CA.pem**).
 - Select choice: **4. Add cert** – this is where you add **CODN_testabc**.
 - » 1. Generate key
 - » 2. Add CA
 - » 3. Generate CSR`
 - » 4. Add cert
 - » 5. List keys
 - » 6. Delete key
 - » 7. List certs
 - » 8. List CA
 - » 9. View CA
 - » 10. Delete CA
 - » 11. Add CRL
 - » 12. Change KDB Password
 - » 13. Add Labeled Password
 - » 14. List Labeled Password
 - » 15. Delete Labeled Password
 - » 16. Import Key Pair
 - » 17. Export Key Pair
 - » 18. Change Label of Key Pair
 - » 19. EXIT
 - » Enter a choice [1 - 19]:

–

BMC CONTROL-M/Agent CONFIG.dat File



› Go to /ctm/data, cat CONFIG.dat

- CTMSHOST testabc
- CTMPERMHOSTS testabc
- ALLOW_COMM_INIT Y
- AGENT_DIR /apps/ctmagent/6.2/ctm
- CMLIST OS
- CM_APPL_TYPE OS
- LOCALHOST testabc
- CODE_VERSION 610
- PROTOCOL_VERSION 06
- FD_NUMBER DRKAI.6.2.01
- DBGLVL 0
- **PERSISTENT_CONNECTION Y**
- ATCMNDATA 2350/120
- AGCMNDATA 2351/120
- TRACKER_EVENT_PORT 2352
- AR_AG_COMM_PORT 2353/120
- AR_AT_COMM_PORT 2354/120
- AR_UT_COMM_PORT 2355/120
- WATCHDOG_ENABLED Y
- **COMMOPT SSL=Y**
- **LISTEN_INTERFACE testabc**

This flag allows blocking
bi-directional firewall access

Note: BMC provides CLIs that simplify editing these configuration files

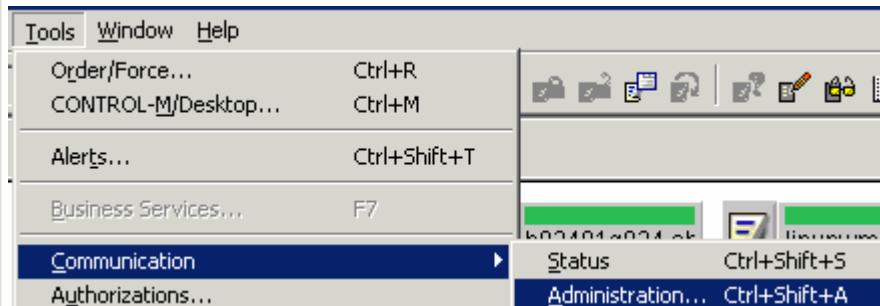
Update Identity on BMC CONTROL-M/Agent



- testabc% vi ag.plc
- [server]
- **identity=AGDN_testabc**
- logfile=agsrv.log
- security_level=3

- [client]
- **identity=AGDN_testabc**
- logfile=agcln.log
- keyfile=/apps/ctmagent/6.2/ctm/data/SSL/cert/agkey.kdb


Update the BMC CONTROL-M Definition in BMC CONTROL-M/Enterprise Manager



CONTROL-M Definitions

Enable

General

 **Name:** UNIX **Code:** ABC

Platform: UNIX/Windows/TAN **Version:** 620


Time Zone: (GMT-06:00) Central Time (US & Canada)

Start Day of the Week: Monday **Day Time:** + 07:00

Daylight Saving Starts: 8/20/2006 Ends: 8/20/2006


CONTROL-R Installed

Communication

 **Protocol:** SSL_ENABLE **TCP/IP Port Number:** 1234


TCP/IP Host Name: testabc

Details

 **Description:** |

Contact: |

Gateway

 **TCP/IP Host Name:** **Port Number:**

OK Cancel

Updating the BMC CONTROL-M/Server – Secure Sockets Layer Set to ENABLED



- > CONTROL-M Main Menu
- > -----
- > Select one of the following menus:
- > 1 - CONTROL-M Manager
- > 2 - Database Creation
- > 3 - Database Maintenance
- > 4 - Database Mirroring
- > 5 - Security Authorization
- > **6 - Parameter Customization**
- > 7 - Node Group
- > 8 - View NodeID details
- > 9 - Agent Status
- > 10 - Troubleshooting
- > q - Quit

> Enter option number ---> [6]:6

Parameter Customization Menu

Select one of the following options:

- 1 - Basic Communication and Operational Parameters
- 2 - Advanced Communication and Operational Parameters
- 3 - System Parameters and Shout Destination Tables**
- 4 - Default Parameters for Communicating with Agent Platforms
- 5 - Parameters for Communicating with Specific Agent Platforms
- q - Quit

Enter option number ---> [q]:3

```

+-----+
| CONTROL-M System Maintenance Utility |
|           Main Menu                 |
+-----+
    
```

- 1) Shout Destination Tables
- 2) System Parameters**
- q) Quit

Enter Option:2

CONTROL-M System Parameters (Page 1/2)

n) Next Page

- s) Save and Return to Main Menu
- c) Cancel

Enter command, or item number you wish to change [n]:n

CONTROL-M System Parameters (Page 2/2)

- 6) Maximum Days Retained by CONTROL-M Log :2
- 7) Maximum Days to Retain Sysout Files :3
- 8) Ignore New Day Conditions :N
- 9) Secure Sockets Layer :ENABLED**

- p) Previous Page
- s) Save and Return to Main Menu
- c) Cancel

Enter command, or item number you wish to change [p]:



- Access files use e-mail fields in server certificates for authentication. Access files can be defined for BMC CONTROL-M/Server and BMC CONTROL-M/Agent.
- Below is the default access file:
 - » [SSL_SERVER]
 - » :
 - » ALLOW_ACL = *
 - » DENY_ACL
- The Allow_ACL or DENY_ACL can be updated with specific e-mail information.

