



MSE System and Appliance Hardening Guidelines

This appendix describes the hardening of MSE, which requires some services and processes to be exposed to function properly. This is referred to as MSE Appliance Best Practices. Hardening of MSE involves disabling unnecessary services, upgrading to the latest server versions, and applying appropriate restrictive permissions to files, services, and endpoints.

This chapter contains the following sections:

- [Setup Wizard Update, page 1](#)
- [Certificate Management, page 3](#)
- [HA Certificate Install Script, page 10](#)
- [Updated Open Port List, page 10](#)
- [Syslog Support, page 11](#)
- [MSE and RHEL 5, page 11](#)

Setup Wizard Update

This section describes the configuration options that have been included in the Setup.sh script and contains the following topics:

- [Configuring Future Restart Day and Time](#)
- [Configuring the Remote Syslog Server to Publish MSE Logs](#)
- [Configuring the Host Access Control Settings](#)

Configuring Future Restart Day and Time

The Mobility Services Engine will restart in a year (or 6 months if DoD mode is enabled) from its last start time. By default, this will happen on a Saturday at 1:00 AM. You can change this default behavior by specifying the future restart day and time using the Future Restart Time option under the setup scripts.

Configuring the Remote Syslog Server to Publish MSE Logs

Use this option to configure a remote syslog server by specifying the IP address, priority parameter, priority level, and facility. You can configure syslog server using either IPv4 or IPv6 address.

Example:

```
A Remote Syslog Server has not been configured for this machine.
Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)se default [Skip]:
y
Configure Remote Syslog Server IP address: 283.12.13.4

Configure Remote Syslog Server Priority parameter.
select a priority level
1)ERROR (ERR)
2)WARNING
3)INFO
Enter a priority level (1-3) :2
Configure Remote Syslog Server's Facility parameter.
Select a logging facility
  KERN(0), // Kernel messages
  USER(1), // user-level messages
  MAIL(2), // mail system
  DAEMON(3), // system daemons
  AUTH(4), // security/authorization messages (note 1)
  SYSLOG(5), // messages generated internally by syslogd
  LPR(6), // line printer subsystem
  NEWS(7), // network news subsystem
  UUCP(8), // UUCP subsystem
  CRON(9), // clock daemon (note 2)
  SECURITY(10), // security/authorization messages (note 1)
  FTP(11), // FTP daemon
  NTP(12), // NTP subsystem
  LOGAUDIT(13), // log audit (note 1)
  LOGALERT(14), // log alert (note 1)
  CLOCK(15), // clock daemon (note 2)
  LOCAL0(16), // local use 0 (local0)
  LOCAL1(17), // local use 1 (local1)
  LOCAL2(18), // local use 2 (local2)
  LOCAL3(19), // local use 3 (local3)
  LOCAL4(20), // local use 4 (local4)
  LOCAL5(21), // local use 5 (local5)
  LOCAL6(22), // local use 6 (local6)
  LOCAL7(23); // local use 7 (local7)

Enter a facility(0-23) :4
```

Configuring the Host Access Control Settings

You can use this option to add, delete, or clear the hosts for accessing the MSE.

Example:

```
Enter whether or not you would like to change the iptables for this machine (giving access
to certain host).
Configure Host access control settings ? (Y)es/(S)kip [Skip]: y
Choose to add/delete/clear host for access control(add/delete/clear): add
Enter IP address of the host / subnet for access to MSE : 258.19.35.0/24 (Rewrite the IP)
For more information on the Setup.sh script, see the Cisco 3350 Mobility Services Engine Getting Started
Guide.
```

Certificate Management

Currently, MSE ships with self-generated certificates. For establishing the trust in an SSL connection establishment, MSE either uses a valid Cisco certificate authority (CA) issued certificate or allows importing a valid CA-issued server certificate. To accomplish this, a command-line interface based CertMgmt.sh is used to import server and CA certificates.

To access the CertMgmt.sh script file, go to the following folder:

```
/opt/mse/framework/bin/
```

This section describes the tasks you can perform using the CertMgmt.sh script and contains the following topics:

- [Creating a CSR](#)
- [Importing the CA Certificate](#)
- [Importing Server Certificate](#)
- [Enabling or Disabling Client Certificate Validation](#)
- [Configuring Online Certificate Status Protocol \(OCSP\) Settings](#)
- [Importing a CRL](#)
- [Clearing Certificate Configuration](#)
- [Showing Certificate Configuration](#)

Creating a CSR

Use this option to create a Certificate Signing Request. The output of this request is the Server Certificate Signing Request and Key. You need to copy the Server CSR and paste it into the certificate authority's website to generate a CA certificate.

Example:

```
Certificate Management Options
    1: Import CA Certificate
    2: Import Server Certificate
    3: Enable Client Certificate Validation
    4: Disable Client Certificate Validation
    5: OCSP Settings
    6: Import a CRL
    7: Create a CSR (Certificate Signing request)
    8: Clear Certificate Configuration
    9: Show Certificate Configuration
   10: Exit
Please enter your choice (1-10)
7
Enter the directory in which the CSR needs to be stored:/root/TestFolder
Enter the Key size: 2048
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/root/TestFolder/mserverkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
```

```

Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:IN
State or Province Name (full name) [Berkshire]:State
Locality Name (eg, city) [Newbury]:City
Organization Name (eg, company) [My Company Ltd]:xyz
Organizational Unit Name (eg, section) []:ABCD
Common Name (eg, your name or your server's hostname) []:example-mse
Email Address []:user@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password123
An optional company name []:abc
The CSR is in: /root/TestFolder/mseservercsr.pem
The Private key is in: /root/TestFolder/mseserverkey.pem

```

Importing the CA Certificate

The certificate authority sends the CA certificate based on the server CSR and the private key you submitted.

Use the Import CA Certificate option to import a CA certificate.

Example:

```

Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
1
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the CA certificate file /root/TestFolder/CACert.cer
Successfully transferred the file
Import CA Certificate successful

```

Importing Server Certificate

After obtaining the CA certificate, you need to obtain the server certificate. Then you need to append the private key information toward the end of the server certificate.

Use the Import Server Certificate option to import a server certificate.

Example:

```

Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings

```

```

        6: Import a CRL
        7: Create a CSR (Certificate Signing request)
        8: Clear Certificate Configuration
        9: Show Certificate Configuration
       10: Exit
Please enter your choice (1-10)
2
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the server certificate file /root/TestFolder/ServerCertUpdated.cer
Successfully transferred the file
Enter pass phrase for /var/mse/certs/exportCert.cer:
Enter Export Password:
Verifying - Enter Export Password:
Enter password for PKCS12 file:
pk12util: PKCS12 IMPORT SUCCESSFUL
Validation is Successful
Import Server Certificate successful

```

Enabling or Disabling Client Certificate Validation

The CA certificate that you obtain from the certificate authority is also copied to the associated clients.

Use this option to enable or disable client certificate validation.

Example:

```

Certificate Management Options
    1: Import CA Certificate
    2: Import Server Certificate
    3: Enable Client Certificate Validation
    4: Disable Client Certificate Validation
    5: OCSP Settings
    6: Import a CRL
    7: Create a CSR (Certificate Signing request)
    8: Clear Certificate Configuration
    9: Show Certificate Configuration
   10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done

Certificate Management Options
    1: Import CA Certificate
    2: Import Server Certificate
    3: Enable Client Certificate Validation
    4: Disable Client Certificate Validation
    5: OCSP Settings
    6: Import a CRL
    7: Create a CSR (Certificate Signing request)
    8: Clear Certificate Configuration
    9: Show Certificate Configuration
   10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done

```

Configuring Online Certificate Status Protocol (OCSP) Settings

Use this option to configure the Online Certificate Status Protocol (OCSP) settings. You are prompted to enter the OCSP URL and default name. In other words, you are asked to provide the URL and default name for the certificate authority.

Example:

```

Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
5
Enter the OCSP URL :
http://ocsp.227.104.178.224
Enter the default ocsp name :ExampleServer

```

Importing a CRL

Use this option to import a certificate revocation list (CRL) which you obtained from the website of the certificate authority.

Example:

```

Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
6
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the CRL file /root/TestFolder/Sample.crl
Successfully transferred the file
Import CRL successful

```

Clearing Certificate Configuration

Use this option to clear the certificate configuration.

Example:

```

Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
8
httpd (no pid file) not running

```

```
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```

Showing Certificate Configuration

Use this option to display the certificate configuration details.

Example:

```
Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OSCP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
9

Certificate Nickname                                     Trust Attributes
                                                         SSL,S/MIME,JAR/XPI

CA-Cert1296638915                                       CT,,
Server-Cert                                              u,u,u
=====
***** Certificates in the database *****
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      74:a1:38:25:75:94:a5:9a:43:2d:4a:23:bd:82:bc:e5
    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Issuer: "CN=ROOTCA1"
    Validity:
      Not Before: Tue Nov 16 18:49:25 2010
      Not After : Mon Nov 16 18:59:25 2015
    Subject: "CN=ROOTCA1"
    Subject Public Key Info:
      Public Key Algorithm: PKCS #1 RSA Encryption
      RSA Public Key:
        Modulus:
          da:06:43:70:56:d8:41:ec:69:e6:65:ad:c5:3b:04:0b:
          cb:cd:83:7c:5f:6e:8f:aa:17:50:6b:6a:3a:48:35:a6:
          65:8a:47:91:48:2f:93:2b:d8:53:6b:33:5c:a9:c2:b2:
          33:c2:fc:9c:55:25:19:d0:79:23:3f:66:60:24:04:ce:
          a3:08:c7:60:f0:b0:8d:b1:31:71:f5:b9:3f:17:46:1a:
          fd:3d:c9:3b:9f:bf:fe:a3:8d:13:52:aa:6b:59:80:43:
          f8:24:e7:49:10:ca:54:6c:f7:aa:77:04:4b:c2:3f:96:
          8d:a1:46:e8:16:1e:a8:e6:86:f4:5c:a0:e5:15:eb:f8:
          5a:72:97:f9:09:65:84:f6:a5:0b:a3:c6:ab:a9:9e:61:
          07:5a:8d:b1:af:93:3b:68:53:8a:5d:f0:14:6e:02:e4:
          38:d2:31:29:5e:a2:1a:93:de:a0:bd:44:9b:05:fd:7b:
          5f:59:23:a1:47:97:87:84:dd:0e:9f:0a:09:cd:df:34:
          b9:6f:9c:b5:4d:07:23:8b:a5:27:16:cd:75:5a:6e:f1:
          c1:5b:6b:21:3a:fd:d9:4d:72:b4:d6:dc:37:86:c2:e3:
          60:56:69:3c:52:27:19:bf:4c:0c:ea:6e:34:29:8c:cf:
          17:50:b3:31:cc:86:1e:32:dc:40:58:92:26:88:58:63
        Exponent: 65537 (0x10001)
    Signed Extensions:
      Name: Certificate Key Usage
      Usages: Digital Signature
              Certificate Signing
              CRL Signing
```

```

Name: Certificate Basic Constraints
Critical: True
Data: Is a CA with no maximum path length.

Name: Certificate Subject Key ID
Data:
    30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
    8e:61:49:eb

Name: Microsoft CertServ CA version
Data: 0 (0x0)

Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
Signature:
    d6:35:b9:27:1f:5b:1a:12:9d:41:a3:16:3a:3a:08:ba:
    91:f4:a9:4b:1b:ff:71:7c:4e:74:16:36:05:04:37:27:
    d0:73:66:a2:47:50:0d:b3:fa:b1:34:dc:36:b8:a9:0a:
    2d:5c:84:35:30:51:4f:7b:55:47:00:53:73:40:c8:95:
    a9:82:83:32:06:ed:0c:95:6d:b1:13:08:3a:e3:cc:88:
    40:9f:e6:43:8c:36:88:e4:a1:91:3e:20:74:29:bf:91:
    25:c1:ef:bc:10:bb:cb:be:08:2c:64:2d:41:a1:3f:81:
    48:ed:80:ed:97:68:6d:83:30:e2:c8:90:ce:45:3a:45:
    cc:78:3c:c4:af:62:73:6a:29:60:c7:70:b1:4c:84:43:
    77:2d:9c:b9:13:dc:9c:b5:8c:74:62:7b:8e:41:ed:37:
    b8:2c:c0:3b:0c:49:cf:61:40:cc:2c:22:74:b2:6b:50:
    e8:31:c9:5f:b8:04:dd:39:7a:9a:46:5e:ee:5a:e8:6a:
    4b:75:97:69:7e:fc:7f:9d:9f:df:f0:3f:06:62:79:77:
    d9:a8:49:a6:00:bf:93:61:00:aa:55:11:26:92:f4:c2:
    8a:61:21:80:af:ef:ab:22:11:ee:10:79:15:4b:1a:8f:
    ae:55:c5:61:03:8e:db:1a:3e:5a:6f:a6:6d:3e:5b:a4
Fingerprint (MD5):
    31:54:A0:D3:A7:40:1A:1E:95:8E:8A:D9:EC:70:47:35
Fingerprint (SHA1):
    F5:72:62:5C:46:AB:2A:5D:7A:75:DA:CB:44:E6:38:76:E0:9E:17:C3

Certificate Trust Flags:
SSL Flags:
    Valid CA
    Trusted CA
    Trusted Client CA
Email Flags:
Object Signing Flags:

Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        4d:a9:34:de:00:00:00:00:00:0b
    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Issuer: "CN=ROOTCA1"
    Validity:
        Not Before: Wed Feb 02 22:40:44 2011
        Not After : Thu Feb 02 22:50:44 2012
    Subject: "E=abc@example.com,CN=abc-mse,OU=XYZ,O=Companyo,L=City,S
        T=State,C=IN"
    Subject Public Key Info:
        Public Key Algorithm: PKCS #1 RSA Encryption
        RSA Public Key:
            Modulus:
                a8:7b:2f:57:94:53:fc:90:c9:37:cb:9a:b3:f6:f4:b8:
                02:04:f3:f8:d8:e1:d1:23:d4:62:7b:30:05:d2:b0:da:
                17:88:b0:22:d5:a6:04:c6:66:fc:64:54:ff:78:5b:f9:
                ef:05:3a:3e:ec:b8:01:7c:3c:9b:78:ac:1d:7f:fb:3b:
                39:f5:31:d2:a2:27:d8:d1:ee:2e:77:98:04:bb:7c:f6:
                0b:9c:ea:15:12:cf:3d:1c:b8:57:63:df:2b:00:48:25:
                32:e4:58:9a:e1:ff:80:5d:2c:24:75:e2:06:de:e6:ae:
                03:7e:c5:f6:e7:97:4d:c1:ad:19:4f:47:20:6c:8d:7a:
                60:75:85:34:3e:ed:f3:1a:77:65:e2:7a:18:e1:17:3d:
                bd:62:1a:1c:4a:d9:49:c3:93:2e:6a:69:fc:e8:87:1e:
                dc:69:11:63:f1:17:63:41:e4:8d:1e:19:3c:e8:80:a9:
                6b:04:c8:18:fb:c9:fe:9d:77:71:30:d2:87:46:82:49:
                0a:1d:ed:4d:ad:66:ad:65:6f:fb:b2:6a:31:45:33:59:
                a7:04:3a:2d:72:f7:55:02:fa:99:02:d9:dd:5e:21:4b:

```



```

                2c:c9:3e:cc:a4:a0:dd:4c:4f:7f:be:45:a7:dd:a9:c4:
                ad:bc:a9:25:a6:1f:53:b8:d0:98:4a:b7:c3:41:a3:d7
                Exponent: 65537 (0x10001)
Signed Extensions:
  Name: Certificate Subject Key ID
  Data:
    bc:a3:66:c6:19:07:56:0a:90:7a:b1:1a:ea:37:17:20:
    74:b8:f1:f5

  Name: Certificate Authority Key Identifier
  Key ID:
    30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
    8e:61:49:eb

  Name: CRL Distribution Points
  URI: "http://win-bncnizib5e2/CertEnroll/ROOTCA1.crl"
  URI: "file://WIN-BNCNIZIB5E2/CertEnroll/ROOTCA1.crl"

  Name: Authority Information Access
  Method: PKIX CA issuers access method
  Location:
    URI: "http://win-bncnizib5e2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
    Al.crt"
  Method: PKIX CA issuers access method
  Location:
    URI: "file://WIN-BNCNIZIB5E2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
    Al.crt"

Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
Signature:
aa:13:74:0d:d1:8c:85:cc:3d:8f:35:c7:e5:9b:a6:4c:
f8:8b:12:a0:12:9f:dc:0a:0a:b5:40:12:eb:05:a9:2b:
65:c5:a3:22:62:1f:47:cd:dd:0f:b8:03:11:a5:63:23:
64:a7:f8:8b:ec:d4:21:dc:d8:22:de:52:75:d9:fb:23:
d4:14:35:d8:78:b7:e2:23:75:05:b4:d0:09:e0:55:ec:
96:8c:22:23:fb:86:74:71:69:ac:03:57:b6:ec:14:a9:
f9:99:b3:98:4c:00:69:e2:26:f8:7b:e9:a0:2a:c2:f4:
6a:75:fc:d1:08:d6:5b:76:93:7a:2c:21:8b:83:ab:52:
a0:85:16:f1:38:35:01:8d:21:34:60:b7:82:39:a7:42:
e7:5f:1a:b7:9d:bf:54:ee:27:97:ba:f8:ca:31:d4:35:
67:55:36:02:b4:48:ab:16:ee:0f:65:56:48:51:de:aa:
9f:7d:35:9b:eb:58:3a:0c:4a:8a:ae:3a:18:47:e3:11:
7b:82:b3:fb:88:94:df:85:82:23:0b:07:46:12:2c:d0:
dd:a7:91:c0:e1:4c:e7:38:9e:34:30:9b:b6:db:c6:8d:
03:df:6e:6b:27:76:da:31:50:44:cd:c8:21:30:42:3c:
75:dc:99:d2:6b:91:9e:bd:b0:5c:8a:52:6b:92:41:0f
Fingerprint (MD5):
77:73:3C:D6:B9:2E:F2:AA:C4:A6:7E:9F:60:D7:55:F7
Fingerprint (SHA1):
60:F8:DC:D2:75:BA:D9:35:4D:21:60:CA:90:EF:09:67:FF:D0:DC:CF

Certificate Trust Flags:
  SSL Flags:
    User
  Email Flags:
    User
  Object Signing Flags:
    User

***** CRLs in the database *****
None
***** Client Certification Settings *****
Client Certificate Validation is disabled
***** OCSP Setting *****
OCSP URL :
http://ocsp.227.104.178.224
OCSP nick name :ExampleServer
=====

```

HA Certificate Install Script



Note

This feature is introduced in 8.0.x.x Release.

A primary and secondary MSE uses self-signed certificates for HA connection. You have the option to install a CA signed certificate for MSE server through another script CertMgmt.sh. You can either use the same CA signed certificate for HA connection or use the `installHACert.sh` script.

The script is available at: `/opt/mse/health-monitor/bin/installHACert.sh`. To execute the script, invoke the it with no arguments.

Prerequisites For Executing the HA Certificate Install Script

- HA is configured for both the primary and secondary MSE.
- MSE is not running on both the servers.
- CA-signed MSE certificate is already installed on both servers using the `CertMgmt.sh` script.
- FIPS mode or Root Access Control (RCA) is disabled on the primary MSE.

Points to Remember:

- The script needs to be executed separately on both the primary and secondary MSE.
- This script needs to be executed after every time a new signed certificate is installed on either the primary or secondary MSE.
- This script requires credentials of the other server of HA pair for secure file copy. Keep the credentials ready.

Sample output from the Primary MSE:

Actual IP addresses are masked in the sample output PPP.PPP.PPP.PPP = Primary MSE's IP address
 SSS.SSS.SSS.SSS = Secondary MSE's IP address On "USERID:" prompt, user needs to enter the user-id of the other MSE of the HA pair. (secondary in this case) On the "PASSWD:" prompt, user needs to enter the password of the above user-id. Password is not displayed on the screen. ----- Sample Output Begin
 ----- # /opt/mse/health-monitor/bin/installHACert.sh Installing HA certificate on MSE (IP = PPP.PPP.PPP.PPP) with role = PRIMARY Press ENTER to continue: We need to import Certificate of SECONDARY MSE server (SSS.SSS.SSS.SSS) to this server using SCP. Please enter user id and password of the SECONDARY MSE server. USERID: root PASSWD: spawn /usr/bin/scp
 root@SSS.SSS.SSS.SSS:/var/mse/certs/ssl/server.crt /var/mse/certs/ha/peer.crt root@SSS.SSS.SSS.SSS's
 password: server.crt 100% 1127 1.1KB/s 00:00 Peer certificate file copied successfully. Installing HA certificates ... Certificates imported successfully.

Updated Open Port List

As part of the non-user requirement, MSE listens on HTTP (8880) and HTTP (8843) ports.

The following are the open ports for MSE:

TCP	80, 443, 22, 8001
	4096, 1411, 4000X (x=1,5)
UDP	162, 12091, 12092

Syslog Support

To ensure compliance with DoD requirements, wIPS supports syslog messaging. The syslog for wIPS is located at `/opt/mse/logs/wips`. This log contains information about wIPS Service, Service start/stop logs, DB logs and error logs. For detailed debug logs, you should turn on `MAJOR_DEBUG` on the wIPS logs .

MSE and RHEL 5

The MSE OS is based on Red Hat Enterprise Linux (RHEL) 5 and the current version of RHEL supported by MSE OS is 5.4. If you are using RHEL 5.3 or earlier, then download and update the openssl patches. Upgrade to RHEL5.4 supports OpenSSH Version 4.3p2-82.el5(which addresses the vulnerabilities in 4.3p2-26.el5_2.1).

