Cisco TelePresence Supervisor MSE 8050 2.3(1.38)

Software Maintenance Release Notes
January 2015

Contents

Product documentation

The following documents provide guidance on installation, initial configuration, and operation of the product:

- Cisco TelePresence Supervisor MSE 8050 Getting started

New features in 2.3

- Conversion of media port and TS screen licenses
- Mutual authentication
- Certificate-based login
- QoS tagging support for administration packets
- Configurable headers and footers
- Web interface changes

Conversion of media port and TS screen licenses

This release introduces an optional feature that allows you to temporarily convert media port licenses to TS screen licenses and vice versa. For example, you can allocate media port licenses to a Cisco TelePresence Server 7010 Blade (up to the port limit of the blade), thus temporarily converting the media port licenses to TS screen licenses. Licenses are converted with a ratio of 1 TS-screen license to 5 media port licenses. Conversions round up to meet the required number of licenses.

This feature requires the “TS screen migration option” feature key. Contact your Cisco representative for advice on obtaining this feature key. To enable the feature, you install the feature key in the **License key management** section on the **Port licenses > License summary** page.

64-character user IDs

Supervisor can now accept and store usernames that are 64 Unicode characters long. This applies anywhere that the Supervisor can accept a username, that is, from the web interface, an API call, or a client certificate's common name.

Tighter password security

Supervisor never stores passwords in plain text. They are always hashed using the SHA-1 algorithm before they are stored, even if an unhashed password is provided in a configuration file.

Changing passwords is also more secure now irrespective of whether or not advanced security mode is enabled. When a user password changes, all session cookies associated with that username will immediately expire. Any users who are logged in when their passwords change will be logged out and may only log in with the new password.

Mutual authentication

Supervisor now supports certificate-based user authentication over HTTPS using mutual TLS authentication between certificates on the user (client) side and certificates held in an HTTPS trust store on Supervisor. Certificates are managed through the new **Network > SSL certificates** page.

Chained certificates are supported. Supervisor checks the client certificate chain against its own trust store; if the certificate is trusted, Supervisor can optionally also perform an OCSP (Online Certificate Status Protocol) check of the leaf certificate.

Certificate-based login

Certificate-based login can be configured as an optional or required alternative to password-based login. With certificate-based login, Supervisor MSE 8050 checks the usernames in its configuration file for a match to the common name in the client certificate. If a match exists, the user who presents the certificate is automatically logged in without entering a username and password.

CAUTION: When setting certificate-based authentication options for Supervisor, it is possible inadvertently to block all login access (including administrators) to the application. If you decide to implement certificate-based authentication, we strongly recommend that you first review the topics “**Configuring SSL certificates**” and “**Transitioning to certificate-based security**” in the Supervisor online help.

Table 1: Certificate authentication options, listed from lowest to highest security level:

1	**Not required**	Default. No client-side authentication is required and certificates are irrelevant to Supervisor. All incoming connections are permitted, even if the remote end does not present a valid and trusted certificate (the remote end is always trusted). Password-based login is the sole authentication mechanism over all user interface connection methods (HTTPS, HTTP, FTP, and the console serial port).
2	**Verify certificate**	Incoming HTTPS connections are only permitted if the remote end has a trusted certificate. Password-based login is required over HTTPS. Password-based login is allowed as normal over HTTP, FTP, and console connections.

Table 1: Certificate authentication options, listed from lowest to highest security level: (continued)

3	**Certificate-based authentication allowed**	Incoming HTTPS connections are only permitted if the remote end has a trusted certificate. Certificate-based login is allowed over HTTPS. If the certificate common name matches a username, the user is logged in automatically. If no match exists, password-based login is required instead. Password-based login is allowed as normal over HTTP, FTP, and console connections.
4	**Certificate-based authentication required**	Incoming HTTPS connections are only permitted if the remote end has a trusted certificate. Certificate-based login is required over HTTPS *and* all other connection types. No password login is allowed and HTTP, FTP, and console connections are effectively disabled (except for functions that do not require login).

Effect of certificate-based user authentication on the API

If certificate-based login is allowed, the standard authentication parameters (**`authenticationUser`** and **`authenticationPassword`**) are required in API messages only if the client certificate is insufficient for login purposes. If certificate-based login is required, the parameters are ignored altogether and a client certificate must be used for login purposes, meaning only HTTPS access is possible.

OCSP checking

Supervisor optionally supports OCSP (using SHA-1 hashing) for real-time checking of HTTPS client certificate revocation status against a pre-configured server. If the status response from the OCSP server is anything other than 'good', Supervisor rejects the certificate and prevents authentication. OCSP settings can be configured to require nonce inclusion, and to define clock skew limits and acceptable ages for OCSP records.

Static Certificate Revocation Lists are not supported.

CAUTION: If you enable OCSP checking for Supervisor, it is possible inadvertently to block all login access (including administrators) to the application. If you decide to implement OCSP checking, we strongly recommend that you first review the topics "**Configuring SSL certificates**" and "**Transitioning to certificate-based security**" in the Supervisor online help.

QoS tagging support for administration packets

This release allows administrators to set their own values for Quality of Service (QoS) bits for administration data packets, including HTTP, HTTPS, FTP, DNS, syslog, OCSP, and NTP traffic.

QoS is set as a six-bit binary value that can be interpreted by networks as either Type of Service (ToS) or Differentiated Services (DiffServ). The online help provides more information about setting the QoS bits.

Configurable headers and footers

Header and footer text (up to 100 characters each) can now be configured for the web user interface. Headers and footers will appear on all pages except the online help.

Web interface changes

- Network Routes and DNS web pages have been updated. The DNS preference drop-down menu is renamed to "DNS configuration", and routes lists are rearranged and split into"IPv4 routes" and "IPv6 routes".
- The Supervisor has a new **Network > QoS** page to manage QoS tagging of data packets.

- The Supervisor has a new **Network > Connectivity** page that enables administrators to 'ping' other devices.
- The Supervisor has new help topics that provide more information on the new and updated UI pages.

Miscellaneous Changes

- Web status pages (such as **Status > General** or **Hardware > Blades**) no longer auto-refresh by default. You can manually specify an auto-refresh interval on the **Settings > User interface** page.

Resolved and open issues in 2.3(1.38)

Use the links below to find up-to-date information about issues resolved since version 2.3(1.32), and open issues in this version, in the Cisco Bug Search Tool.

Issue Type	Link
Resolved Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283645291&rls=2.3%281.38%29&sb=fr&srtBy=byRel&bt=custV
Open Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283645291&rls=2.3%281.38%29&sb=afr&srtBy=byRel&bt=custV
Resolved and open issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283645291&rls=2.3%281.38%29&sb=anfr&srtBy=byRel&bt=custV

Resolved since 2.3(1.31)

Identifier	Description
CSCuo21584	**Symptom:** Cisco TelePresence Supervisor MSE 8050 includes a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration and running software release 2.3(1.31) are affected by this vulnerability. Releases prior to 2.3(1.31) are not affected by this vulnerability. **Workaround:** Not currently available. Customers that do not require the new functionality nor bug fixes provided on release 2.3(1.31) may evaluate the possibility of downgrading affected devices to release 2.2(1.17). **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved since 2.2(1.17)

Identifier	Description
CSCub32234	In some circumstances, the Supervisor stopped responding to HTTP(S) requests on both the web interface and API calls. This recent problem has been attributed to Firefox browser version 14.0.1 (the first release code of Firefox 14; release date: 17th July 2012) and is improved in this release. This version of Firefox is still not recommended; Firefox 15 should be used instead (release date: 28th August 2012). See also the Limitations [p.5] section of these release notes.

Limitations

Firefox 14 is not supported for use with the MSE 8050. We strongly recommend that you refrain from using Firefox 14 to access the Supervisor web interface. This version of the browser causes an issue that was not present in previous browser versions and which has been fixed in the following version (Firefox 15).

Upgrading to version 2.3

Prerequisites and software dependencies

The software upgrade requires a restart of the hardware. Notify any users who may be affected by a temporary loss of service.

Back up the Supervisor's configuration before you start – you may need to roll back your upgrade.

CAUTION: You must back up your configuration before upgrading to version 2.3.

You must also remember the administrator user name and password for the backup configuration. You will need these if you ever need to make use of this backup file.

We also recommend that you back up the audit logs.

Upgrade instructions

1. Unzip the image file
2. Browse to the IP address of the MSE 8050
3. Log in as an administrator
4. Go to **Settings > Upgrade**
5. In the **Main software image** section, type in, or browse to the software image file
6. Click **Upgrade software image**
   The web browser uploads the file and displays a progress window. Do not navigate away from or refresh the web page during upload.
   When the upload completes, the status window displays an upload success message.
7. Close the status window
8. The web interface reminds you that you need to restart the Supervisor to complete the upgrade
9. Click the **Shutdown** button, then click the **Confirm** button
10. Click the **Restart** button
    The Supervisor upgrades itself using the software image you uploaded, and the browser displays a restart in progress message.
11. Wait for a few minutes and then go to the status page to check the software version. You may need to log in again

Note: If you have been logged out due to inactivity, log in again as admin, go to **Settings > Shutdown**, and then click Restart MSE Supervisor and upgrade to complete the upgrade.

The progress of the upgrade can be monitored through the serial port.

Downgrade instructions

If you need to reverse your upgrade, you can re-install the former version of the software.

Note: We do not support downgrading to MSE 8050 versions earlier than 2.0. The compulsory password protection included from that version onwards makes it impossible to log in to the MSE 8050 after a downgrade to an earlier version. If you are experiencing these circumstances, visit the Cisco support website.

The downgrade procedure is the same as the upgrade procedure except you will use the earlier software image.

You need the correct version of the software and your saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image
2. Restart the hardware and check the status via the web interface
   The status report indicates the software version.
3. Restore your configuration from the saved XML file

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Technical support

If you cannot find the answer you need in the documentation, check the website at www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document revision history

Table 2: Supervisor release notes revisions

Date	Revision	Description
January 2015	06	Second maintenance release of Cisco TelePresence Supervisor MSE 8050. Version 2.3(1.38)
May 2014	05	First maintenance release of Cisco TelePresence Supervisor MSE 8050. Version 2.3 (1.32)
December 2012	04	These notes accompany the release of Cisco TelePresence Supervisor MSE 8050, version 2.3(1.31)