Oracle® ILOM Security Guide For Firmware Releases 3.x and 4.x

Part No: E37451-21
December 2019

Oracle ILOM Security Guide For Firmware Releases 3.x and 4.x

Part No: E37451-21

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Référence: E37451-21

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** — This guide provides web and CLI information about Oracle ILOM security tasks and guidelines. Use this guide in conjunction with other guides in the Oracle ILOM Documentation Library.
- **Audience** — Technicians, system administrators, and authorized Oracle service providers who have experience managing system hardware.
- **Required Knowledge** — Experience with configuring and managing Oracle servers.

Product Documentation Library

Documentation and resources for this product and related products are available at `http://www.oracle.com/goto/ilom/docs`.

Feedback

Provide feedback about this documentation at `http://www.oracle.com/goto/docfeedback`

Security Features Per Oracle ILOM Firmware Release

Use the following table to identify the firmware release in which an Oracle ILOM security feature became available.

Firmware Version Availability	Security Feature	For details, see:
All	Authentication and Authorization	■ "Securing Oracle ILOM User Access" on page 27
All	Dedicated Secure Management Connection	■ "Securing the Physical Management Connection" on page 17 ■ "Maintaining a Secure Management Connection" on page 63
All	Encrypted Preconfigured Network Ports	■ "Preconfigured Services and Network Ports" on page 21
All	IPMI 2.0 Secure Management	■ "Configure IPMI Management Access for Increased Security" on page 58
All	Secure Shell Key Encryption Configuration	■ "Use Server Side Keys to Encrypt SSH Connections" on page 54 ■ "Append SSH Keys to User Accounts for Automated CLI Authentication" on page 55
All	SNMP 3.0 Secure Management	■ "Configure SNMP Management Access for Increased Security" on page 56
All	SSL Protocols and Certificates	■ "Upload a Custom SSL Certificate and Private Key to Oracle ILOM" on page 46 ■ "Obtain a Custom SSL Certificate and Private Key Using OpenSSLToolkit" on page 45 ■ "Enable the Strongest TLS Encryption Properties" on page 49
All	Remote Console Encryption and Secure Protocols	■ "Using Remote KVMS Securely" on page 66
3.0.4 and later	KVMS Host Lock Configuration	■ "Lock Host Access Upon Exiting a KVMS Session" on page 36
3.0.4 and later	Session Timeout Configuration	■ "Set a Timeout Interval for Inactive Web Sessions" on page 50 ■ "Set a Timeout Interval for Inactive CLI Sessions" on page 52

Firmware Version Availability	Security Feature	For details, see:
3.0.12 and later	Local Host Interconnect Authenticated Sessions	■ “Preferred Authenticated Host Interconnect Access” on page 64
3.0.8 and later	Login Banner Configuration	“Secure System Access With Login Banner (3.0.8 and later)” on page 38
3.0.8 to 3.1.2	WS-Management Secure Access	■ “Configure WS-Management Access for Increased Security” on page 62
3.1.0 and later	Separate Audit Log	■ “Monitor Audit Events to Find Unauthorized Access” on page 72
3.1.0 and later	Physical Security Presence Check	■ “Physical Security Presence for Resetting `root` Account Default Password” on page 70
3.2.4 and later	IPMI 1.5 Configurable Property	■ “Configure IPMI Management Access for Increased Security” on page 58
3.2.4 and later	TLS Protocol Versions 1.1 and 1.2	■ “Enable the Strongest TLS Encryption Properties” on page 49
3.2.4 and later	KVMS Sessions Count	■ “Limit Viewable KVMS Sessions for Remote System Console Plus (3.2.4 or later)” on page 37
3.2.4 and later	FIPS Compliance Encryption Support	■ “Choosing Whether to Configure FIPS Mode At Deployment” on page 18 ■ “Unsupported Features When FIPS Mode Is Enabled” on page 20 ■ “Post Deployment Considerations for Securing User Access” on page 69
3.2.5 and later	SSH Server State and Weak Ciphers	■ “Management of SSH Server State and Weak Ciphers ” on page 52
3.2.5 and later	Password Policy for Local User Accounts	■ “Set Password Policy Restrictions for All Local Users (3.2.5 and later)” on page 32
3.2.6 and later Later versions of 3.2.4.x and 3.2.5.x	The Weak Ciphers property for SSH Management Access was removed. The Weak Ciphers and SSL properties for HTTPS Management Access was removed.	■ “Management of SSH Server State and Weak Ciphers ” on page 52 ■ “Enable the Strongest TLS Encryption Properties” on page 49
3.2.8 and later	New TLS management service over IPMI.	■ “Configure IPMI Management Access for Increased Security” on page 58
3.2.8 and later	New Default web interface (self-signed) SSL Certificate behavior.	■ “Regenerate Self-Signed Default SSL Certificate Issued By Oracle” on page 42
3.2.9 and later	The TLSv 1.0 property is disabled by default.	■ “Enable the Strongest TLS Encryption Properties” on page 49
4.0.0	New ASR Endpoint SSL Certificate behavior.	■ “Securing the Automatic Service Request (ASR) Endpoint Connection” on page 39
4.0.0	Support for TLS v1.0 service is removed.	■ “Enable the Strongest TLS Encryption Properties” on page 49
4.0.0	The `servicetag` protocol, when in use, should be configured to use HTTPS and a passphrase.	■ Table 6, “Impact of Services When Enabled or Disabled,” on page 23

Firmware Version Availability	Security Feature	For details, see:
4.0.4	The TLSv 1.1 property is disabled by default.	■ "Enable the Strongest TLS Encryption Properties" on page 49

Additional Security Information

For additional information about securing Oracle ILOM, see the following sections in this guide:

- "Checklists for Keeping Oracle ILOM Secure" on page 13
- "Oracle ILOM Deployment Practices for Increasing Security" on page 17
- "Oracle ILOM Post Deployment Practices for Increasing Security" on page 63

Checklists for Keeping Oracle ILOM Secure

Oracle Integrated Lights Out Manager (ILOM) is a preinstalled service processor (SP) on all Oracle servers and most legacy Sun servers. System administrators use Oracle ILOM's user interfaces to perform remote server management tasks, as well as real-time server health monitoring operations.

To ensure that proper security practices for Oracle ILOM are implemented in your environment, system administrators should consult the security tasks listed in the following checklists:

- "Security Checklist for Server Deployment" on page 13
- "Security Checklist for Post Server Deployment" on page 14

Related Information

- "Oracle ILOM Deployment Practices for Increasing Security" on page 17.
- "Oracle ILOM Post Deployment Practices for Increasing Security" on page 63
- "Security Features Per Oracle ILOM Firmware Release" on page 9

Security Checklist for Server Deployment

To determine which Oracle ILOM security practices might be best when planning the deployment of a new server, system administrators should consult the list of security tasks recommended in the following Table 1, "Checklist - Configuring Oracle ILOM Security at Server Deployment ," on page 13.

TABLE 1 Checklist - Configuring Oracle ILOM Security at Server Deployment

✓	Security Task	Applicable Firmware Version(s)	For details, see:
	Establish a secure dedicated management connection to Oracle ILOM.	All firmware versions	▪ "Securing the Physical Management Connection" on page 17

✓	**Security Task**	**Applicable Firmware Version(s)**	**For details, see:**
	Decide whether FIPS 140-2 security compliance is required at or after deployment; or, not at all.	Firmware versions 3.2.4 and later	■ "Choosing Whether to Configure FIPS Mode At Deployment" on page 18 ■ "Unsupported Features When FIPS Mode Is Enabled" on page 20
	Set Password Policy for All Local User Accounts	Firmware version 3.2.5 and later	■ "Set Password Policy Restrictions for All Local Users (3.2.5 and later)" on page 32
	Modify the default password provided for the preconfigured Administrator `root` account.	All firmware versions	■ "Avoid the Creation of Shared User Accounts" on page 27 ■ "Modify Default Password for `root` Account at First Login" on page 33
	Decide whether the preconfigured Oracle ILOM services and their open network ports are applicable for your target environment.	All firmware versions	■ "Securing Services and Open Network Ports" on page 21
	Configure user access to Oracle ILOM.	All firmware versions	■ "Securing Oracle ILOM User Access" on page 27 ■ "Create Local User Accounts With Role-Based Privileges" on page 35
	Decide whether access to the host operating system should be locked upon exiting a remote KVMS session.	Firmware versions 3.0.4 and later	■ "Lock Host Access Upon Exiting a KVMS Session" on page 36
	Decide whether to limit other SP users from viewing remote KVMS sessions launched from the SP.	Firmware versions 3.2.4 and later	■ "Limit Viewable KVMS Sessions for Remote System Console Plus (3.2.4 or later)" on page 37
	Decide whether to display a security banner message at user login or immediately following user login.	Firmware versions 3.0.8 and later	■ "Secure System Access With Login Banner (3.0.8 and later)" on page 38
	Ensure that the proper security properties are set for all Oracle ILOM user interfaces.	All firmware versions	■ "Configuring Oracle ILOM Interfaces for Increased Security" on page 41
	For ASR Client configurations, choose to keep the preinstalled SSL Certificate or upload a user-specified SSL Certificate.	Firmware versions 4.0.x and later.	■ "Securing the Automatic Service Request (ASR) Endpoint Connection" on page 39
	Ensure that the `servicetag`protocol is properly configured to use HTTPS and a passphrase.	Firmware versions 4.0.x and later.	■ Table 6, "Impact of Services When Enabled or Disabled," on page 23

Security Checklist for Post Server Deployment

To determine which Oracle ILOM security practices are best to maintain on existing servers in your environment, system administrators should consult the list of security tasks recommended in the following Table 2, "Checklist - Maintaining Oracle ILOM Security After Server Deployment ," on page 15.

TABLE 2 Checklist - Maintaining Oracle ILOM Security After Server Deployment

✓	**Security Task**	**Applicable Firmware Version(s)**	**For details, see:**
	Maintain a secure management connection to Oracle ILOM	All firmware versions	■ "Avoid Unauthenticated Host KCS Device Access" on page 63 ■ "Preferred Authenticated Host Interconnect Access" on page 64 ■ "Configure IPMI Management Access for Increased Security" on page 58
	Ensure that remote KVMS and serial text-based sessions are securely launched from Oracle ILOM.	All firmware versions	■ "KVMS Remote Communication and Encryption" on page 67 ■ "Protect Against Remote KVMS Shared Access" on page 67 ■ "Protect Against Host Serial Console Shared Access" on page 68
	Maintain and track user access to Oracle ILOM.	All firmware versions	■ "Post Deployment Considerations for Securing User Access" on page 69
	Security actions required for resetting a lost password for the preconfigured Admin `root` account.	Firmware versions 3.1 and later	■ "Physical Security Presence for Resetting `root` Account Default Password" on page 70
	Security actions required if the FIPS 140-2 compliance mode must be modified in Oracle ILOM after server deployment.	Firmware version 3.2.4 and later	■ "Modify FIPS Mode Post Deployment" on page 73 ■ "Unupported Features When FIPS Mode Is Enabled" on page 20
	Ensure your software and firmware are current on the server.	All firmware releases	■ "Updating to the Latest Software and Firmware" on page 75

Oracle ILOM Deployment Practices for Increasing Security

Use the following topics to decide the best Oracle ILOM deployment practices to implement at server deployment.

- "Securing the Physical Management Connection" on page 17
- "Choosing Whether to Configure FIPS Mode At Deployment" on page 18
- "Securing Services and Open Network Ports" on page 21
- "Securing Oracle ILOM User Access" on page 27
- "Securing the Automatic Service Request (ASR) Endpoint Connection" on page 39
- "Configuring Oracle ILOM Interfaces for Increased Security" on page 41

Related Information

- "Checklists for Keeping Oracle ILOM Secure" on page 13.
- "Oracle ILOM Post Deployment Practices for Increasing Security" on page 63
- "Security Features Per Oracle ILOM Firmware Release" on page 9

Securing the Physical Management Connection

Oracle ILOM is an out-of-band (OOB) management tool that uses a dedicated management channel for maintaining and monitoring Oracle servers. Unlike servers with in-band management tools, Oracle servers arrive with built-in remote management capabilities, enabling system administrators to gain secure access to Oracle ILOM through a separate dedicated network connector on the service processor. While Oracle ILOM's management functionality provides system administrators with specific capabilities for monitoring and managing Oracle servers, Oracle ILOM is not designed to be a general-purpose compute engine, or accessed from an unsecured, non-trusted network connection.

Whether or not you establish a physical management connection to Oracle ILOM through the local serial port, dedicated network management port, or the standard data network port, it is essential that this physical port on the server or chassis monitoring module (CMM) is always connected to an internal trusted network, or a dedicated secure management or private network. For further guidelines when establishing a physical management connection to Oracle ILOM, see the following table.

Physical Port Management Connection to Oracle ILOM	**Supported Oracle Hardware**	**Management Connection Security Guidelines**
Dedicated Connection	- Server (Port: `NET MGT`) - CMM (Port: `NET MGT`)	Use a dedicated internal network for the service processor (SP) to separate it from the general data network traffic. For further details, about establishing a dedicated network management connection to Oracle ILOM, see - Dedicated Network Management Connection, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)*
Local Connection	- Server (Port: `SER MGT`) - CMM (Port: `SER MGT`)	Use a local serial management connection to access Oracle ILOM directly from the physical server or CMM. For further details about establishing a local serial management connection to Oracle ILOM, see: - Local Serial Network Management Connection to Oracle ILOM, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)*
Sideband Connection	Server (Ports: `NET0, NET1`, `NET2`, `NET3`)	Use a shared Ethernet data network to access the service processor SP whenever it is necessary to simplify cable management and network configuration by preventing the need for two separate network connections. For further details about establishing a sideband management connection to Oracle ILOM, see - Sideband Management Connection, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)* **Note -** Sideband management is supported on most Oracle servers.

Note - To defend against security attacks, **you should never connect the Oracle ILOM SP to a public network**, such as the Internet. You should keep the Oracle ILOM SP management traffic on a separate management network and grant access only to system administrators.

Choosing Whether to Configure FIPS Mode At Deployment

As of Oracle ILOM firmware release 3.2.4, the Oracle ILOM CLI and web interface provide a configurable mode for Federal Information Processing Standards (FIPS) Level 1 compliance.

When this mode is enabled, Oracle uses cryptographic algorithms in compliance with the FIPS 140-2 security standards for protecting system sensitive or valuable data.

System administrators deploying servers with firmware 3.2.4 or later should decide whether to configure FIPS mode prior to configuring other Oracle ILOM properties. By default, the FIPS compliance mode in Oracle ILOM is shipped disabled. Changes to the FIPS compliance mode will cause all configuration data to be reset to their factory default values.

To enable FIPS mode compliance at deployment (prior to configuring Oracle ILOM properties), see "Enable FIPS Mode at Deployment" on page 19. In the case where user-defined configuration properties have already been set in Oracle ILOM and you need to modify the FIPS property, see "Post Deployment Actions for Modifying FIPS Mode" on page 72.

▼ Enable FIPS Mode at Deployment

Note - FIPS compliance mode in Oracle ILOM is represented by State and Status properties. The State property represents the configured mode in Oracle ILOM and the Status property represents the operational mode in Oracle ILOM. When the FIPS State property is changed, the change does not affect the operational mode (FIPS Status property) until the next Oracle ILOM reboot.

Before You Begin

- The FIPS State and Status properties are shipped disabled by default.
- When FIPS is enabled (configured and operational) some features in Oracle ILOM are not supported. For a list of unsupported features when FIPS is enabled, see Table 3, "Unsupported Features in Oracle ILOM When FIPS Mode Is Enabled," on page 21.
- The Admin (a) role is required to modify the FIPS State property.
- The configurable property for FIPS compliance is available in Oracle ILOM as of firmware 3.2.4 or later. Prior to firmware release 3.2.4, Oracle ILOM does not provide a configurable property for FIPS compliance.
- All user-defined configuration settings are reset to their factory defaults upon modifying the FIPS mode State and Status properties in Oracle ILOM.

1. **In the Oracle ILOM web interface click ILOM Administration -> Management Access -> FIPS.**

2. **In the FIPS page, perform the following:**

   a. **Select the FIPS State check box to enable the configured FIPS property.**

b. Click Save to apply the change.

For additional configuration details, click the `More details`.... link on the FIPS web page.

3. To change the FIPS operational mode status in Oracle ILOM, perform the following steps to reboot Oracle ILOM.

a. In the web interface, click ILOM Administration -> Maintenance -> SP Reset.

b. In the SP Reset page, click the SP Reset button.

Upon rebooting Oracle ILOM, the following occurs:

- The last configured FIPS State (enabled) is applied on the system.
- Any user-defined configuration settings previously configured in Oracle ILOM are reset to their factory default values.
- The FIPS Status property is updated to reflect the current enabled operational state in Oracle ILOM.

  For a complete list and description of the FIPS Status messages, click the `More details` link on the FIPS page.
- A FIPS shield icon appears in the masthead area of the web interface.
- All non-supported FIPS features are either disabled or removed from the CLI and web interface.

  For a complete list and description of non-supported FIPS features, click the `More details` link on the FIPS page.

Related Information

- "Unupported Features When FIPS Mode Is Enabled" on page 20
- "Post Deployment Actions for Modifying FIPS Mode" on page 72
- Configure FIPS Mode Properties, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)*.

Unupported Features When FIPS Mode Is Enabled

Upon enabling FIPS compliance in Oracle ILOM, the following non-compliant FIPS 140-2 features in Oracle ILOM are not supported.

TABLE 3 Unsupported Features in Oracle ILOM When FIPS Mode Is Enabled

Unsupported FIPS Mode Feature	Description
IPMI 1.5	When FIPS mode is enabled and running on the system, the IPMI v1.5 configuration property is removed from the Oracle ILOM CLI and web interface. IPMI TLS service and the IPMI v2.0 service support both FIPS complaint and non-compliant modes.
Firmware Compatibility for Oracle ILOM System Remote Console	FIPS mode in Oracle ILOM prevents the earlier firmware versions of Oracle ILOM Remote System Console to be compatible with the later Oracle ILOM remote System Console firmware versions. For instance, the Oracle ILOM Remote System Console client firmware version 3.2.4 is backward compatible with the Oracle ILOM Remote System Console firmware version 3.2.3 and earlier. However the Oracle ILOM Remote System Console client firmware version 3.2.2 and earlier are not forward compatible with the Oracle ILOM Remote System Console firmware version 3.2.4 and later. **Note -** This firmware compatibility limitation does not apply to the Oracle ILOM Remote System Console Plus. The Oracle ILOM Remote System Console Plus is provided on newer service processor systems such as SPARC T5 and later systems, and or Oracle Server x4-4, x4-8 and later systems. The Oracle ILOM Remote System Console is provided on older service processor systems such as SPARC T3 and T4 and Sun Server x4-2/2L/2B and earlier systems.
Lightweight Directory Access Protocol (LDAP)	When FIPS mode is enabled and running on the system, the LDAP configuration properties in Oracle ILOM are automatically removed from the Oracle ILOM CLI and web interface. **Note -** The following remote authentication services are supported in both FIPS compliant and non-compliant modes: Active Directory and LDAP/SSL.
Remote Authentication Dial-In User Service (RADIUS)	When FIPS mode is enabled and running on the system, the RADIUS configuration properties in Oracle ILOM are automatically removed from the Oracle ILOM CLI and web interface. **Note -** The following remote authentication services are supported in both FIPS compliant and non-compliant modes: Active Directory and LDAP/SSL.
Simple Network Management Protocol (SNMP) DES and MD5	When FIPS mode is enabled and running on the system, the SNMP configuration properties for DES Privacy Protocol and MD5 Authentication Protocol are not supported in the Oracle ILOM CLI or web interface.

Securing Services and Open Network Ports

To ensure that services and their respective network ports are properly configured in Oracle ILOM, refer to the following topics:

- "Preconfigured Services and Network Ports" on page 21
- "Management of Unwanted Services and Open Ports" on page 22
- "Configuring Services and Network Ports" on page 24

Preconfigured Services and Network Ports

Oracle ILOM comes preconfigured with most services enabled by default. This makes the deployment of Oracle ILOM simple and straightforward. However, each open service network port on the server represents a potential attach point by a malicious user. It is therefore important to understand the initial Oracle ILOM settings, and their purpose, and to choose which services are actually required for a deployed system. For best security, enable only the required Oracle ILOM services.

The following table lists the services that are enabled by default with Oracle ILOM.

TABLE 4 Services and Ports Enabled by Default

Service	Port(s)
HTTP redirection to HTTPS	80
HTTPS	443
IPMI TLS client connections **Note -** IPMI TLS client connections are supported as of Oracle ILOM firmware 3.2.8 and later.	623 (TCP)
IPMI LAN and LANPLUS client connections	623 (UDP)
Remote KVMS for Oracle ILOM Remote Console	5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579
Remote KVMS for Oracle ILOM Remote Console Plus (Oracle ILOM firmware 3.2.2 and later)	443
Remote KVMS for Oracle ILOM Remote Console Plus (Oracle ILOM firmware prior to 3.2.2)	5120, 5555
Service Tag	6481
SNMP	161
Single Sign-on	11626
SSH	22

The following table shows the services that are disabled by default with Oracle ILOM.

TABLE 5 Services and Ports Disabled by Default

Service	Port(s)
HTTP	80

Management of Unwanted Services and Open Ports

All Oracle ILOM services can be optionally disabled, which results in the closing of the respective open network ports for those services. While most services are enabled by default, you might want to disable some features or change default settings to make the Oracle ILOM environment more secure. Any Oracle ILOM service can be disabled, but will result in the loss of features. As a general rule, enable only those services that are absolutely necessary in the deployed environment. The loss of features must be weighed against the security benefit of having fewer network services enabled.

The following table describes the impact of enabling or disabling each service.

TABLE 6 Impact of Services When Enabled or Disabled

Service	Description	Result of Enabling/Disabling
HTTP	A non-encrypted protocol for accessing the Oracle ILOM web interface	Enabling this service provides faster performance than encrypted HTTP (HTTPS). However, using this protocol might result in sensitive information being sent over the Internet without encryption.
HTTPS	An encrypted protocol for accessing the Oracle ILOM web interface	Enabling this service provides secure communication between a web browser and Oracle ILOM. However, because it requires having an open network port on Oracle ILOM, there is an increase in vulnerability to an attack, such as Denial of Service. **Note -** If you need to disable the HTTPS service and your system supports the Oracle ILOM Remote System Console Plus, disabling the HTTPS service (port 443) is not enough. For systems supporting the Oracle ILOM Remote System Console Plus, both the HTTPS and KVMS services must be disabled. For systems supporting the Oracle ILOM Remote System Console, you can disable the HTTPS service (port 443) only.
Servicetag	An Oracle discovery protocol used to identify servers and facilitate service requests	The Servicetag property is enabled by default and is configurable from the Oracle ILOM CLI. Disabling this service makes it impossible for Oracle Enterprise Manager Ops Center to discover Oracle ILOM, and prevents integration into other Oracle automatic service solutions. **Note - Sensitive Data Warning**: When enabled, the Servicetag service uses the HTTP protocol by default, which is a clear text protocol that does not encrypt sensitive data. To encrypt sensitive data when using the Oracle ILOM Servicetag service, configure the Servicetag CLI property with a passphrase and use HTTPS as a communication method. For configuration information, see "Servicetag Service Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*.
IPMI	A standard management protocol	Disabling this service might prevent Oracle Enterprise Manager Ops Center, as well as some Oracle management connectors to third-party software, from managing the system.
SNMP	A standard management protocol for monitoring the health of Oracle ILOM and monitoring received trap notifications	Disabling this service might prevent Oracle Enterprise Manager Ops Center, as well as some Oracle management connectors to third-party software, from managing the system.
KVMS	A set of protocols for providing remote keyboard, video, mouse, and storage	Disabling this service makes the host console and remote storage functionality unavailable, preventing their use of the Oracle ILOM Remote System Console (or Oracle ILOM Remote System Console Plus) and CLI Storage Redirection applications.

Service	Description	Result of Enabling/Disabling
SSH	A secure protocol for accessing a remote shell	Disabling this service disallows command-line access over the network and might prevent Oracle Enterprise Manager Ops Center from discovering Oracle ILOM.
SSO	A single sign-on feature that reduces the number of times a user has to enter a user name and password	Disabling this service prevents launching KVMS without having to re-enter a password and allows drill-down from a chassis monitoring module (CMM) to a blade SP without having to re-enter a password.

For information about enabling and disabling individual network services, see the following topic "Configuring Services and Network Ports" on page 24.

Configuring Services and Network Ports

For instructions on how to configure management services and their respective network ports in Oracle ILOM, see the following procedures.

- "Modify Protocol Management Service States and Ports" on page 24
- "Modify the KVMS Service State and Ports" on page 25
- "Modify the Single Sign-On Service State and Port" on page 26

You can disable or enable services and their respective network ports by using the Oracle ILOM command-line interface (CLI) or web interface. The procedures in this section provide web-based navigation instructions for all Oracle ILOM firmware releases. For CLI instructions or for additional details about configuration properties, refer to the appropriate documentation listed in the Related Information section that follows each procedure.

▼ Modify Protocol Management Service States and Ports

Before You Begin

- Review the following tables to determine which protocol services and network ports are enabled or disabled by default in Oracle ILOM.
  - Table 4, "Services and Ports Enabled by Default," on page 22 Services and Ports Enabled by Default
  - Table 5, "Services and Ports Disabled by Default," on page 22 Services and Ports Disabled by Default
- The Admin (a) role is required in Oracle ILOM to modify the State property of protocol services.

Follow these steps to modify the State property of a network service.

1. **In the Oracle ILOM web interface navigate to the Management Access services.**

For instance, in the:

- **3.0.x web interface, click Configuration -> System Management Access.**
- **3.1 and later web interface, click ILOM Administration -> Management Access.**

2. **Click the appropriate Management Access -> service tab listed below:**

Management Access ->	Description
Web Server	Use the Web Server page to manage the service state and port assignments for HTTP and HTTPS protocol management access.
IPMI	Use the IPMI page to manage the service state and port properties for IPMI protocol management access.
SNMP	Use the SNMP page to manage the service state and port properties for SNMP management access.
SSH	Use the SSH page to manage the service state property for secure shell management access.

3. **Modify the State property on the Management Access -> service page, and then click Save to apply the change.**

Note that disabling the State property of a protocol service results in closing the respective protocol service network port, and preventing the use of the protocol service with Oracle ILOM.

Related Information

- Management Services and Network Default Properties, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Management Services and Network Default Properties, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Configuring Network Settings, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Configuring Network Settings, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

▼ Modify the KVMS Service State and Ports

Before You Begin

- The KVMS service State property is enabled by default in Oracle ILOM. For a list of the open network ports that are associated with the KVMS service, see Table 4, “Services and Ports Enabled by Default,” on page 22.

- The Admin (a) role is required to modify the KVMS State property in Oracle ILOM.

Note - The Oracle ILOM KVMS consoles require the Java Runtime Environment to be either Java 7 update131 or later, Java 8, or Java 9. All Java versions support v1.2. However, if a version prior to Java 7u131 is installed, you will need to manually enable TLS v1.2 , or update your system with a later Java version. To download the latest Java Runtime Environment, go to http://java.com.

Note - As of Oracle ILOM 4.0.0, TLS v1.0 is not supported. As of Oracle ILOM 4.0.4, TLS v1.1 is disabled by default. TLS v1.2 is enabled by default.

---

1. **Navigate to the KVMS tab in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click Remote Control -> KVMS.**

   - **3.1 and later web interface, click Remote Console -> KVMS.**

2. **In the KVMS tab modify the KVMS State property, and then click Save to apply the change.**

   Note that disabling the State property results in closing the respective open KVMS service network ports; thereby preventing the use of: a) the remote host console, and b) the Oracle ILOM Remote Console and the Oracle ILOM Remote Storage CLI; or the Oracle ILOM Remote Console Plus.

Related Information

- Configure Local Client KVMS Settings, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Configure Local Client KVMS Settings, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Initial Setup Tasks, *Oracle ILOM 3.0 Remote Redirection Console - Web and CLI Guide*

▼ Modify the Single Sign-On Service State and Port

Before You Begin

- The Single Sign-On (SSO) service State property and respective network port (1126) is enabled by default in Oracle ILOM.

- The User Management (u) role is required in Oracle ILOM to modify the SSO service State property.

1. **Navigate to the User Account tab in the Oracle ILOM web interface.**
   For instance, in the:

   - **3.0.x web interface, click User Management -> User Account.**

   - **3.1 and later web interface, click ILOM Administration -> User Account.**

2. **In the User Account page modify the SSO State property, and then click Save to apply the change.**
   Note that disabling the SSO State property in Oracle ILOM results in: a) closing the open SSO network port; b) prompting users to re-enter their password upon launching a KVMS console; and c) allowing CMM users to navigate to a blade server SP without having to re-enter password.

Related Information

- Single Sign-On Service, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Single Sign-On Service, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Configure Single Sign-On, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Configure Single Sign-On, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Securing Oracle ILOM User Access

To secure user access in Oracle ILOM, refer to the following topics:

- "Avoid the Creation of Shared User Accounts" on page 27
- "Assignment of Role-Based Privileges" on page 28
- "Security Guidelines for Managing User Accounts and Passwords" on page 29
- "Remote Authentication Services and Security Profiles" on page 31
- "Configuring User Access for Increased Security" on page 32

Avoid the Creation of Shared User Accounts

Maintain a secure environment by avoiding the creation of shared accounts. Shared accounts are user accounts that share a given user account password. Instead of creating shared accounts, the ideal method for handling user accounts is to create a unique password for each user who has access to Oracle ILOM. Ensure that each user account and password combination are known only to one user.

Note - Oracle ILOM supports up to 10 local user accounts. If you require more users to access Oracle ILOM, you can configure directory services, such as LDAP or Active Directory, to support more accounts using a centralized database. For more details, see "Remote Authentication Services and Security Profiles" on page 31.

After establishing individual user accounts with unique passwords, the system administrator should ensure that a unique password was assigned to the preconfigured Administrator `root` account. Otherwise, without a unique password, the preconfigured Administrator `root` account is considered a shared account. To ensure that unauthorized users do not use the preconfigured Administrator `root` account, you must modify the password or remove the preconfigured `root` account from Oracle ILOM. For further details about the preconfigured Administrator `root` account, see "Modify Default Password for `root` Account at First Login" on page 33.

For further guidance about establishing secure accounts with unique passwords, refer to the "Security Guidelines for Managing User Accounts and Passwords" on page 29.

For user account configuration information, see "Configuring User Access for Increased Security" on page 32.

Assignment of Role-Based Privileges

All Oracle ILOM user accounts are assigned a set of role-based privileges. These role-based privileges provide access to discrete features within Oracle ILOM. It is possible to configure a user account so that the user can monitor the system but cannot make any configuration changes. Or, you can allow a user to modify most configuration options, with the exception of creating and modifying user accounts. It is also possible to restrict who can control the server power and who can access the remote console. It is important to understand the privilege levels and to assign them appropriately to users in the organization.

The following table defines a list of privileges you can assign to an individual Oracle ILOM user account.

TABLE 7 User Account Privilege Descriptions

Role	Description
`Admin (a)`	Enables a user to change all Oracle ILOM configuration options, except for those configuration options expressly authorized by other privileges (such as User Management).

Role	Description
`User Management (u)`	Enables a user to add and remove users, change user passwords, and configure authentication services. A user with this role can create a second user account with all privileges and, therefore, this role has the highest level of privileges of all user roles.
`Console (c)`	Enables a user to access the host console remotely. This remote console access might allow the user to access the BIOS or OpenBoot PROM (OBP), which gives the user the ability to change boot behavior as a way to gain access to the system.
`Reset and Host Control (r)`	Enables a user to control host power and reset Oracle ILOM.
`Read-only (o)`	Enables a user to have read-only access to the Oracle ILOM user interfaces. All users have this access, which entitles a user to read logs and environmental information, as well as view configuration settings.

For more information about creating a local user account and assigning role-based privileges, see "Create Local User Accounts With Role-Based Privileges" on page 35.

Security Guidelines for Managing User Accounts and Passwords

Consider the following security guidelines when managing Oracle ILOM user accounts and passwords:

- "Guidelines for User Account Management" on page 29
- "Guidelines for Password Management" on page 30

Guidelines for User Account Management

User Account Management Guideline	Description
Never Promote the Sharing of User Accounts	A separate account should always be created for each Oracle ILOM user. Oracle ILOM supports a Increased of 10 local user account. If you are managing a larger site and require more than 10 user accounts, you should consider using a third-party user authentication service such as LDAP or Active Directory. For more information about implementing user authentication in Oracle ILOM through an external authentication service, see "Remote Authentication Services and Security Profiles" on page 31.
Select Conforming Names for Local User Accounts	When selecting a user name for a local Oracle ILOM user account, the user name must: ■ Contain from 4 to 16 characters in length (the first character must be a letter). ■ Be unique across your organization ■ Not contain spaces, a period (.), or a colon (:)

User Account Management Guideline	Description
Select Conforming Passwords for Local User Accounts	When selecting a password for a local Oracle ILOM user account, the password must: ■ Always be a strong password that contains a Increased of 16 characters in length ■ Contain a mixture of lowercase and uppercase characters, as well as one or two special characters to create a strong complex password ■ Not contain spaces, a period(.) or a colon(:) ■ Conform to your company's password management policy For further details about password management in Oracle ILOM, see "Security Guidelines for Managing User Accounts and Passwords" on page 29.
Limit User Account Privileges Based on Job Role (*Principles of Least Privilege*)	The principle of least privilege states that, for good security practice, give a user the least amount of privileges to perform his or her job. Over-ambitious granting of responsibilities, roles, and so on (especially early in the life cycle of an organization), can leave a system open for abuse. Review user privileges periodically to determine their relevance to the current job responsibilities of each user. Oracle ILOM provides the ability to control user privileges for each user. Ensure that the appropriate user role permissions are assigned to each user account, based on job role. For details on how to create a user account with role-based privileges, see: "Create Local User Accounts With Role-Based Privileges" on page 35

Guidelines for Password Management

Password Management Guideline	Description
Change the Default `root` Password (`changeme`) Immediately After Initial Login	To enable first-time login and access to Oracle ILOM, a local Administrator `root` account is provided with the system. To build a secure environment, you must change the provided Administrator password (`changeme`) after your initial login to Oracle ILOM. Gaining unauthorized access to the Administrator `root` account gives a user unrestricted access to all features of Oracle ILOM. Therefore, it is essential to specify a strong, secure password.
Change All Oracle ILOM Account Passwords on a Regular Basis	To prevent malicious activity and ensure that passwords remain in accordance with current password policies, you should change all Oracle ILOM passwords on a regular basis.
Enforce Common Practices for Creating Strong Complex Passwords	Enforce the following common practices for creating strong complex passwords: ■ Do not create a password that is shorter than 16 characters in length. ■ Do not create a password that contains the user name, employee name, or family member names. ■ Do not select passwords that are easy to guess. ■ Do not create passwords that contain a consecutive string of numbers, such as 12345. ■ Do not create passwords that contain a word or string that is easily discoverable by a simple Internet search. ■ Do not allow users to reuse the same password across multiple systems. ■ Do not allow users to reuse older passwords. ■ For Increased security, you should always mask new password entries in the CLI by using the following syntax:

Password Management Guideline	Description
	set [*SP|CMM***]/users/root password=**[*do not type password, press Enter*] - or- **set [***SP|CMM***]/users/newuser password=**[*do not type password, press Enter*] The CLI will prompt for the new password value, masking the password from view.
Set Password Policy Restrictions for Local Users (Available as of firmware 3.2.5 and later)	Enforce a password policy for all local user accounts. For more details, see "Set Password Policy Restrictions for All Local Users (3.2.5 and later)" on page 32
Consult Your IT Security Officer for Password Management Policies	Consult your IT Security Officer to ensure that your company's password management requirements and policies are being met.

Remote Authentication Services and Security Profiles

Oracle ILOM can be configured to use an external centralized user store rather than having to configure local users on each Oracle ILOM instance. This provides the added convenience of being able to centrally create and modify user credentials and enable users to gain access to many different systems.

Before choosing and configuring an authentication service, understand how these services work and how each needs to be configured. In addition to authentication, each of the supported services provide the ability to configure authorization rules that define how the Oracle ILOM user privileges get assigned for a given remote user. Ensure that the proper user role or privilege gets assigned.

The following table describes the user authentication services supported by Oracle ILOM.

TABLE 8 Remote Authentication Services and Security Profiles

Service Name	Security Profile	Information
Active Directory	High	■ This service is secure by default. ■ Using strict certification mode requires a certificate server, but adds an additional layer of security.
Lightweight Directory Access Protocol/Secure Socket Layer (LDAP/SSL)	High	■ This service is secure by default. ■ Using strict certification mode requires a certificate server, but adds an additional layer of security.
Legacy LDAP	Low	■ Use this service on private, secure networks where there are no suspected malicious users.
Remote Authentication Dial In User Service (RADIUS)	Low	■ Use this service on private, secure networks where there are no suspected malicious users.

Services with a high security profile can be used in very secure environments as they are secured by certificates and other forms of strong encryption to protect the channel. The services with a low security profile are disabled by default. Enable these low security profiles only if you understand and accept the limitations of this low level of security.

For remote authentication service configuration details, refer to the appropriate Oracle ILOM documentation below:

- Setting Up and Maintaining User Accounts, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Setting Up and Maintaining User Accounts, Oracle ILOM 3.1 *Configuration and Maintenance Guide*
- Managing User Accounts, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Managing User Accounts, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Configuring User Access for Increased Security

Refer to the following topics for how to best configure Oracle ILOM's user access for Increased security.

- "Set Password Policy Restrictions for All Local Users (3.2.5 and later)" on page 32
- "Modify Default Password for `root` Account at First Login" on page 33
- "Create Local User Accounts With Role-Based Privileges" on page 35
- "Lock Host Access Upon Exiting a KVMS Session" on page 36
- "Limit Viewable KVMS Sessions for Remote System Console Plus (3.2.4 or later)" on page 37
- "Secure System Access With Login Banner (3.0.8 and later)" on page 38

You can configure user access properties in Oracle ILOM by using the command-line interface (CLI) or web interface. The procedures in this section provide web-based navigation instructions for all Oracle ILOM firmware releases. For CLI instructions, or for additional details about configuration properties, refer to the appropriate documentation listed in the Related Information section that follows each procedure.

▼ Set Password Policy Restrictions for All Local Users (3.2.5 and later)

Oracle ILOM, as of firmware release 3.2.5, enforces a password policy for all local user accounts. The password policy ships with a default set of password policy restrictions. System administrators can either choose to use the default properties as is or modify them to meet their password policy needs.

Note - Modifications to the password policy properties should be set prior to creating local user accounts. In the event that the Password Policy properties are modified after configuring local user accounts, Oracle ILOM will automatically: 1) remove the configuration of all local user accounts, and 2) restore the default root account that was initially provided with the system.

Before You Begin

- The Admin (a) role is required to configure the Password Policy properties.
- The Password Policy applies only to local user accounts. It has no impact on remote user authentication service accounts like LDAP or Active Directory.
- Upon saving changes to the password policy properties, the following will occur:
  - All local user account configurations are deleted from Oracle ILOM.
  - The default local user account (root) shipped with the system is restored.
  - On the initial log in of root, the root user is prompted to change the root-account password.

Use the following web-based instructions to set a Password Policy for all local users:

Note - For CLI Password Policy instructions, click the Oracle ILOM Administration Guide reference listed in the Related Information section of this procedure.

1. **To view the current Password Policy restrictions in Oracle ILOM, click ILOM Administration > User Management > Password Policy.**

2. **To modify the Password Policy restrictions, click the More Details... link on the Password Policy page for further instructions.**

3. **To save your changes, click Save.**

Related Information

- "Modify Password Policy Restrictions for Local Users" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

▼ Modify Default Password for `root` Account at First Login

To enable first-time login and access to Oracle ILOM, a preconfigured Administrator `root` account and a default password (`changeme`) are provided with the system. To prevent unauthorized access to Oracle ILOM, the default password (`changeme`) that is shipped with the preconfigured root account must be changed at first login. Otherwise, the preconfigured root account and default password (changeme) will act as a shared account, enabling administrator access to any user.

Use the following web-based instructions to modify the default password (changeme) that is shipped with the preconfigured Administrator root account.

Note - If you do not have access to the preconfigured root account and you require access to Oracle ILOM administrator features, contact your system administrator for a user account with administrator privileges.

Before You Begin

- Review the "Security Guidelines for Managing User Accounts and Passwords" on page 29.

  Note - Assigning a strong, secure password to the root account is essential for preventing unauthorized access to Oracle ILOM features. A strong password should contain a combination of lowercase and uppercase characters, and at least one special character such as % or $.

- The User Management (u) role is required to modify local user account passwords in Oracle ILOM.

1. **Navigate to the User Account page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click User Management -> User Accounts.**
   - **3.1 and later web interface, click User Management -> User Accounts.**

2. **In the User Account page, click Edit for the root account.**

   An Edit: User Root dialog appears.

3. **In the Edit: User Root dialog, perform the following:**

   - **Enter a unique password in the New Password text box, then re-enter the same password in the Confirm New Password text box.**
   - **Click Save to apply the change.**

Related Information

- Configuring a Local User Account, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Configuring a Local User Account, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Modify a User Account, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Modify a User Account, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- "Physical Security Presence for Resetting `root` Account Default Password" on page 70

▼ Create Local User Accounts With Role-Based Privileges

Before You Begin Oracle ILOM supports the creation and storage of up to 10 local user accounts on a single SP or chassis monitoring module (CMM). Oracle ILOM users are assigned a set of privileges that enables them to work with features to the extent they are permissible by their configured account.

Note - Alternatively, system administrators can configure Oracle ILOM to support additional user accounts through a remote authentication service. With a remote authentication service configuration, logins, passwords, and privileges are derived from an external user store. For more details, see "Remote Authentication Services and Security Profiles" on page 31.

For web-based instructions for configuring a local user account with role-based access privileges, see the following instructions.

Before You Begin

- Review the "Security Guidelines for Managing User Accounts and Passwords" on page 29.
- Review the Table 7, "User Account Privilege Descriptions," on page 28 Supported Web Browsers for Oracle ILOM.
- The User Management (u) role in Oracle ILOM is required to create a local user account with privileges.

1. **Navigate to the User Account page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click User Management -> User Accounts.**
   - **3.1 and later web interface, click User Management -> User Accounts.**

2. **In the User Account page, click Add.**
   The Add User dialog appears.

3. **In the Add User dialog, perform the following:**

   a. **Specify the name of the user in the User Name text box.**

   b. **In the Roles drop-down list, select the appropriate user role profile (administrator, operator, or advanced).**

   c. **Enter a unique password in the New Password text box, then re-enter the same password in the Confirm New Password text box.**

   d. **Click Save to apply the changes.**

Related Information

- Create User Account and Assign User Role, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Create User Account and Assign User Role, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Add User Account and Assign Roles, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Add User Account and Assign Roles, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

▼ Lock Host Access Upon Exiting a KVMS Session

Because the host console is considered a shared network resource when using Remote KVMS, if one user logs into the host console and closes either the Oracle ILOM Remote System Console, Remote System Console Plus, or the CLI Storage Redirection application without having logged out from the host operating system, a second user who connects to the same console using Remote KVMS will be able to use the previously authenticated operating system session. For this reason, Oracle ILOM provides the ability to automatically lock the host operating system whenever a Remote KVMS session is disconnected. For Increased security, enable or configure this feature in Oracle ILOM.

To lock the remote host desktop after terminating a KVMS sessions, see the following web-based instructions. For information about how to enable the host lock feature, see the *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*.

Before You Begin

- The Console (c) role is required to modify the host lock mode property in Oracle ILOM.
- Firmware 3.0.4 or later is required to use the host lock mode feature in Oracle ILOM.
- The host lock mode feature is disabled by default.

1. **Navigate to the KVMS page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click Remote Console -> KVMS.**
   - **3.1 and later web interface, click Remote Control -> KVMS.**

2. **In the Host Lock Settings section of the KVMS page, perform one of the following.**

   - **Specify a lock mode (Windows, Custom, or Disabled).**
   - **Click Save to apply the change.**

Related Information

- Lock Host Desktop, *Oracle ILOM Administrator Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Lock Host Desktop, *Oracle ILOM 3.1 Configuration and Maintenance*
- KVMS Lock, *Oracle ILOM 3.0 Remote Redirection Consoles CLI and Web Guide*

▼ Limit Viewable KVMS Sessions for Remote System Console Plus (3.2.4 or later)

As of firmware release 3.2.4, a primary Remote System Console Plus user can prevent other signed-in session users on the SP from viewing confidential data entered during a video redirection session by limiting the Maximum Client Session Count to one (1) session viewer. By default, the Maximum Client Session Count property for the Oracle ILOM Remote System Console Plus is set to four sessions viewers.

To modify the Maximum Client Session Count property for the Oracle ILOM Remote System Console Plus, see the following web-based instructions.

Before You Begin

- The KVMS Maximum Client Session Count property for the Oracle ILOM Remote System Console Plus is available as of firmware release 3.2.4 or later.

Note - The KVMS Maximum Client Session Count property is not configurable on systems supporting the Oracle ILOM Remote Console.

- The Oracle ILOM Remote System Console Plus is only available on newly released SP systems as of firmware release 3.2.1.
- The Console (c) role is required in Oracle ILOM to modify the KVMS Maximum Client Session Count property.
- Upon resetting the Maximum Client Session Count property in Oracle ILOM, all active Oracle ILOM Remote System Console Plus video sessions on the SP will be terminated.
- By default, a maximum of four Remote System Console Plus video redirection sessions, per SP, can be launched from the Redirection page in Oracle ILOM.

1. **Navigate to the KVMS page in the Oracle ILOM web interface by clicking Remote Console -> KVMS.**

2. **In the KVMS page, modify the Maximum Client Session Count property (acceptable value:** *4* **(default)|***1***|***2***|***3***).**

3. **Click Save to apply the change.**

Related Information

- Remote Device Redirection Properties, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*

▼ Secure System Access With Login Banner (3.0.8 and later)

As of firmware release 3.0.8 , Oracle ILOM enables system administrators to display a banner message to all users upon logging in to the Oracle ILOM CLI and web interface. The use of a login banner can help protect against unauthorized system access by remote devices, as well as advise authorized and legitimate users of their obligations relating to acceptable use of the system.

The banner message you implement should be written in accordance with your information security policy. For further guidelines about the written message, consult your site administrator or security officer.

To display a banner message to all users at login or post login, see the following web-based instructions.

Before You Begin

- The Admin (a) role is required to create a banner message.

- The banner message is available for configuration as of Oracle ILOM firmware release 3.0.8 and later.
- Administrators can configure the banner message to display on the Login page, or in a dialog that appears immediately after the user logs in to Oracle ILOM.

1. **Navigate to the Banner Message page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click System Information -> Banner Messages.**

   - **3.1 and later web interface, click ILOM Administration -> Management Access -> Banner Messages.**

2. **In the Banner Message page, click the** *More Details...* **link to determine how to configure a banner message.**

   For CLI instructions, refer to the applicable *Oracle ILOM Administration Guide* that is listed in the Related Information section of this procedure.

3. **Click Save to apply your changes.**

Related Information

- "Management of Banner Messages at Log-In" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*
- Management of Banner Messages, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Banner Message Configuration Properties, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Display Banner Message, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Display Banner Message, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Securing the Automatic Service Request (ASR) Endpoint Connection

Oracle ILOM, as of firmware release 4.0, provides SSL Certificate configuration properties for ASR Client configurations. By default, an SSL Certificate is pre-installed for all direct service endpoint client configurations (https://transport.oracle.com). For indirect service endpoint client configurations, a user-specified SSL Certificate must be uploaded to Oracle ILOM.

For further information about uploading an ASR Client SSL Certificate to Oracle ILOM, see the following topic for "Uploading an SSL Certificate for ASR Client Configurations " on page 40.

Uploading an SSL Certificate for ASR Client Configurations

Before You Begin

- Oracle ILOM must be configured as an ASR Client. For ASR Client configuration details, see "Managing Automatic Service Requests" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*.
- The Admin role is required to upload a user-specified SSL certificate for direct and indirect service endpoint configurations.

Note - Administrators can choose to either keep or replace the pre-installed SSL certificate for direct endpoint client configurations (https://transport.oracle.com).

- The following procedure provides web-based instructions for uploading an ASR Client SSL Certificate. For CLI instructions, see "Manage Endpoint SSL Certificate Information" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*.

To upload a user-specified SSL Certificate for ASR direct or indirect client configurations, follow these steps:

1. **In the Oracle ILOM web interface, select the ILOM Administrations → Notifications → ASR Client.**

2. **Select the Strict Certificate Mode checkbox in the General Settings section of the ASR Client page.**

3. **Perform any of the following to locally manage the Endpoint SSL Certificate in Oracle ILOM:**

   - **To view the SSL Certificate**:
     - In the Certificate Information section, view the Certificate File Status. If the status shows the certificate is *present*, click the *(details)* link for further certificate details.
   - **To load the SSL Certificate**:

  - In the Certificate Information section, select a Transfer Method, provide the required information, and then click Load Certificate.

    For more details, see "Supported File Transfer Methods" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*.

- **To remove the SSL Certificate**:
  - In the Certificate Information section, click Remove Certificate.

    A message appears indicating that the certificate was removed.

Configuring Oracle ILOM Interfaces for Increased Security

To configure the Oracle ILOM interfaces for Increased security, refer to the following topics:

- "Configure the Web Interface for Increased Security" on page 41
- "Configure the CLI for Increased Security" on page 51
- "Configure SNMP Management Access for Increased Security" on page 56
- "Configure IPMI Management Access for Increased Security" on page 58
- "Configure WS-Management Access for Increased Security" on page 62

Configure the Web Interface for Increased Security

Refer to the following topics for how to best configure the Oracle ILOM web interface for Increased security.

Note - You can configure the web management interface properties in Oracle ILOM by using the command-line interface (CLI) or web interface. The procedures in this section provide web-based navigation instructions for all Oracle ILOM firmware releases. For CLI instructions, or for additional details about configuration properties, refer to the appropriate documentation listed in the Related Information section that follows each procedure.

- "Improve Security by Using a Trusted SSL Certificate and Private Key" on page 42
- "Enable the Strongest TLS Encryption Properties" on page 49
- "Set a Timeout Interval for Inactive Web Sessions" on page 50

Improve Security by Using a Trusted SSL Certificate and Private Key

Secure Socket Layer (SSL) certificates are used both to encrypt communication over a network and to ensure the authenticity of a server or client. Oracle ILOM includes a self-signed SSL certificate that allows the HTTP over SSL protocol to be used out-of-box, without the need for uploading a certificate. When connecting to the Oracle ILOM web interface for the first time, the user is notified that a self-signed certificate is being used and is asked to accept its use. Using the certificate provided, all communication between the web browser and Oracle ILOM is fully encrypted.

However, it is also possible to create and upload a trusted certificate for improved security. A trusted certificate means that the certificate is granted in conjunction with a trusted certificate authority. Using a trusted certificate from a known Certificate Authority ensures the authenticity of the Oracle ILOM web server. Using untrusted (self-signed) certificates opens up the possibility of a man-in-the-middle (MITM) attack.

To regenerate the self-signed Default SSL Certificate from Oracle or to obtain and upload a custom signed SSL Certificate issued from a Certificate Authority, refer to the following procedure(s).

- “Regenerate Self-Signed Default SSL Certificate Issued By Oracle” on page 42
- “Obtain a Custom SSL Certificate and Private Key Using OpenSSLToolkit” on page 45
- “Upload a Custom SSL Certificate and Private Key to Oracle ILOM” on page 46
  - “Certificate Chain Order” on page 47
- “Validate Custom CA SSL Certificate Configuration in Java Client” on page 48

▼ Regenerate Self-Signed Default SSL Certificate Issued By Oracle

As of firmware version 3.2.8, each Oracle ILOM SP, CMM, and FMM ships with a unique self-signed Default SSL Certificate. The Default SSL Certificate is used by Oracle ILOM whenever a Custom SSL Certificate is not configured.

The unique Default SSL Certificate is initially generated at the factory with a unique host certificate fingerprint value. Oracle ILOM automatically regenerates a new version of the Default SSL Certificate and fingerprint whenever its configuration properties are reset to defaults. System administrators, at any time, can choose to replace the existing Default SSL Certificate and fingerprint with a newer version. For instructions for regenerating the Default SSL Certificate and fingerprint in Oracle ILOM, see the following information.

Before You Begin

- Admin (a) role is required to regenerate the Default SSL Certificate.

- Oracle ILOM firmware version 3.2.8 or later must be in use.
- By default, the Oracle ILOM Default SSL Certificate is generated with a 3072 bit key size. Optionally, you can change default key size (3072) to either 2048 or 4096.
- All Oracle ILOM web interface and KVMS console user connections are immediately disconnected upon regenerating a new Default SSL Certificate.
- When the Default (self-signed) SSL Certificate is used in Oracle ILOM, additional certificate checks will take place to protect Oracle ILOM from man-in-the-middle attacks. For instance:
  - Oracle ILOM remote KVMS console users will be prompted to manually validate the self-signed SSL certificate prior to gaining access to the Oracle ILOM Remote System Console / Remote System Console Plus. To manually validate the self-signed SSL certificate, the user must ensure that the host fingerprint value on the Check Certificate Warning dialog box matches the host fingerprint value issued by Oracle. For additional information about validating the host fingerprint value assigned to the self-signed Default SSL Certificate, see "Resolving Warning Messages for Self-Signed SSL Certificate" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*.

    Note - The host fingerprint value issued by Oracle appears on the Management Access > SSL Certificate web page and the Default Certificate CLI target (`/`*SP*`|`*CMM*`|`*FMM*`/services/https/ssl/default_cert`)

  - A Video Redirection Error dialog box appears when a change to the original Default SSL Certificate and fingerprint is detected. In this case, the user can either edit the local host fingerprint file with the last fingerprint value issued by Oracle or remove the host fingerprint file from the local user directory. Otherwise, the user will be prevented from gaining access to the Oracle ILOM Remote System Console / Remote System Console Plus. For additional information for resolving the Video Redirection Error, see, "Resolving Warning Messages for Self-Signed SSL Certificate" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

    Note - The Certificate Checks described above will not occur when a custom signed SSL Certificate is configured in Oracle ILOM. For instructions on how to obtain and upload a custom signed SSL Certificate, see these topics: "Obtain a Custom SSL Certificate and Private Key Using OpenSSLToolkit" on page 45 and "Upload a Custom SSL Certificate and Private Key to Oracle ILOM" on page 46.

To regenerate the Default (self-signed) SSL Certificate in Oracle ILOM, follow these steps:

1. **In the Oracle ILOM web interface, click ILOM Administration > Management Access > SSL Certificate.**

   The SSL Certificate page appears.

2. **In the Default Certificate section of the SSL Certificate page, perform the following steps:**

   a. **(Optional) To modify the Default SSL Certificate Key Size (3072), click the Key Size list box and select the appropriate key size.**

   b. **To regenerate the Default SSL Certificate and the host fingerprint value, click Create.**

      A message appears confirming that you want to regenerate a new Default SSL Certificate and fingerprint.

3. **In the Confirmation Message dialog box, click OK to proceed.**

4. **View the Create SSL Certificate Results field to track the creation status.**

   For instance, one or more of the following status messages might appear:

   - **Running — This status message appears when Oracle ILOM is in the process of creating a new Default SSL Certificate and fingerprint.**

     Upon creating the new Default SSL Certificate and fingerprint, all Oracle ILOM web interface and KVMS console user connections will be disconnected. KVMS and web interface users can immediately log in to Oracle ILOM after being disconnected.

   - **New Cert Has Been Created — This status message appears after a new Default SSL Certificate was generated by a user.**

   - **Certificate Creation Failed —This status message appears when Oracle ILOM was unable to process the request to create a new Default SSL Certificate and fingerprint.**

   - **(None) — This status message appears when the last Default SSL Certificate was generated by Oracle ILOM, or when a user changed the Default SSL Certificate key size in the ILOM CLI but did not regenerate the Default SSL Certificate.**

Related Information

- For Oracle ILOM CLI SSL Certificate properties, see "SSL Certificate and Private Key Configuration Properties for HTTPS Web Server" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

▼ Obtain a Custom SSL Certificate and Private Key Using OpenSSLToolkit

This procedure is a simplified description on how to obtain a custom SSL Certificate using the OpenSSL toolkit. Your requirement to use a temporary self-signed or a certificate authority-signed certificate should be determined by your site administrator or security officer. In the event you do need to obtain a custom SSL certificate (temporary self-signed or certificate authority-signed), you can follow these example OpenSSL command-line instructions below.

Note - Oracle ILOM does *not* require you to use OpenSSL to generate SSL certificates. OpenSSL is used in this procedure for demonstration purposes only. Other tools are available for generating SSL certificates.

Note - If further OpenSSL instructions are required to generate the SSL certificate, you should consult the user documentation provided with the OpenSSL toolkit.

---

1. **Create a network share or local directory to store the certificate and private key.**

2. **To generate a new RSA private key using the OpenSSL toolkit, type:**

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   Where <*foo*> equals the name of the private key.

   Note - This private key is a 2048 bit RSA key which is stored in a PEM format so that it is readable as ASCII text.

   ---

3. **To generate a certificate signing request (CSR) using the OpenSSL toolkit, type:**

   ```
   openssl req -new -key <foo>.key -out <foo>.csr
   ```

   Where <*foo*> equals the name of the certificate signing request.

   Note - During the generation of the CSR, you will be prompted for several pieces of information.

   A <*foo*>.csr file should now appear in your current working directory.

4. **To generate an SSL certificate, perform one of the following:**

   - **Generate a temporary self-signed certificate (good for 365 days).**

     The self-signed SSL certificate is generated from the `server.key` private key and `server.csr` files.

     Using the OpenSSL toolkit, type:

     ```
     openssl x509 -req -days 365 -in <foo>.csr
     -signkey <foo>.key -out <foo>.cert
     ```

     Where <*foo*> equals the name assigned to the private key (`.key`) or certificate (`.cert`).

   Note - This temporary certificate will generate an error in the client browser to the effect that the signing certificate authority is unknown and not trusted. If this error is unacceptable, you should request the Certificate Authority to issue you a signed certificate.

   - **Obtain an officially signed certificate from a certificate authority provider.**

     Submit your certificate signing request (<*foo*>`.csr`) to an SSL certificate Authority provider. Most certificate authority providers require you to cut and paste the CSR output in a web application screen. It can typically take up to seven business days to receive your signed certificate.

5. **Upload the new SSL certificate and private key to Oracle ILOM.**

   See the following instructions, "Upload a Custom SSL Certificate and Private Key to Oracle ILOM" on page 46.

▼ Upload a Custom SSL Certificate and Private Key to Oracle ILOM

Before You Begin

- Admin (a) role is required to modify the web server properties in Oracle ILOM.
- Obtain the new (temporary self-signed or certificate authority-signed) HTTPS certitude and private key. For instructions using the OpenSSL toolkit, see "Obtain a Custom SSL Certificate and Private Key Using OpenSSLToolkit" on page 45.
- Ensure that you can access the new HTTPS certificate and private key through your network or local file system.
- When uploading a certificate chain for SSL, ensure that the certificates within the certificate chain are listed in the correct order. For more details, see "Certificate Chain Order" on page 47.

1. **Navigate to the SSL Certificate page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click Configuration -> System Management Access -> SSL Certificate.**
   - **3.1 and later web interface, click ILOM Administration -> Management Access -> SSL Certificate.**

2. **In the SSL server page, perform the following;**

   a. **Click the Load Certificate button to upload the Custom Certificate file that is designated in the File Transfer Method properties.**

   b. **Click the Load Custom Private Key button to upload the Custom Private Key file that is designated in the File Transfer Method properties.**

   c. **Click Save to apply the changes.**

3. **If a Certification Authority (CA) SSL Certificate and private key were uploaded to Oracle ILOM, verify that the Java client is properly configured to validate the custom CA SSL certificate that is currently configured in Oracle ILOM. For instructions, see the following procedure "Validate Custom CA SSL Certificate Configuration in Java Client" on page 48.**

Related Information

- SSL Certificate and Private Key Configuration Properties, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- SSL Certificate and Private Key Configuration Properties, *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Upload SSL Certificate, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Upload SSL Certificate, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Certificate Chain Order

An SSL Certificate Chain links your intermediate certificate(s) to the trusted root certificate. When using a certificate chain, the SSL certificates in the chain must be listed in the following order:

1. ilom.cer

2. intermediate.cer(s)
3. root.trusted_CA.cer

Example: Create Certificate Chain

```
cat ilom.cer  intermediate.cer  root_trusted_CA.cer > cer-chain.cer
```

where:

- `cat` represents the Symantec command used in this example to create a certificate chain file (*cer-chain.cer*).
- *ilom.cer* is the sender's certificate, which must come first in list.
- any *intermediate.cer* that follows must directly certify the proceeding certificate.
- *root_trusted_CA.cer* represents the root certificate issued by the Certificate Authority.

Validate Custom CA SSL Certificate Configuration in Java Client

After uploading a custom CA SSL Certificate and private key to Oracle ILOM, perform the following steps to verify that the Java client is properly configured to validate the custom CA SLL certificate and private key.

1. **Verify that the required root CA certificate or intermediate root CA certificate is configured in client side Java keystore. To view the Java keystore, use the keytool command with the `-list` option, for example:**

   - On a Windows system, at the prompt, type:

     ```
     keytool -list -keystore "c:\Program Files (x86)\Java\jre<version>\lib\security
     \cacerts
     ```
   - On a Linux system, at the prompt, type:

     ```
     keytool -list -keystore $JAVA_HOME/jre/lib/security/cacerts
     ```

2. **Locate the alias and/or fingerprint of the root CA certificate or intermediate root CA certificate that is required by the custom CA certificate currently configured in Oracle ILOM, then perform one of the following:**

   - If the required root CA Certificate or intermediate root CA certificate is present in the Java keystore, you can, at any time, proceed to start the Oracle ILOM remote KVMS console at any time.
   - If the required root CA Certificate or intermediate root CA certificate is missing in the Java keystore, consult with your security officer or system administrator prior to continuing this procedure to add the missing the CA certificate details to the Java keystore.

3. **Use the `-importcert` keytool command to add the missing root CA certificate or intermediate root CA certificate to the Java keystore. For example:**

   - On a Windows system, at the prompt, type:

     Note - The `-importcert` command needs to be run an administrator. To start a command prompt as an administrator on a Windows systems: Click Start, click All Programs, and then click Accessories. Right-click Command prompt, and then click Run as administrator.

     ```
     keytool -importcert -alias certalias -file root-ca-cert -keystore "c:\Program Files
     (x86)\Java\jre<version>\lib\security\cacerts"
     ```

   - On a Linux system, at the prompt, type:

     ```
     keytool -importcert -alias certalias -file root-ca-cert -keystore $JAVA_HOME/jre/lib/
     security/cacerts
     ```

4. **Verify that the required root CA certificate or intermediate root CA certificate is now available in the Java keystore using the keytool command with the `-list` and `-alias` options, for example:**

   - On a Windows system, at the prompt, type:

     ```
     keytool -list -alias certalias -keystore "c:\Program Files (x86)\Java\jre<version>
     \lib\security\cacerts"
     ```

   - On a Linux system, at the prompt, type:

     ```
     keytool -list -alias certalias -keystore $JAVA_HOME/jre/lib/security/cacerts
     ```

▼ Enable the Strongest TLS Encryption Properties

The TLS v1.2 encryption configuration property is enabled by default in newer Oracle ILOM firmware releases . Use the following procedure to view or modify the web server security properties in Oracle ILOM.

Before You Begin

- Admin (a) role is required to modify the web server properties in Oracle ILOM.
- The default setting for the TLS protocol properties in Oracle ILOM is dependent on the firmware version that is currently installed on the managed device. For instance:
  - TLS v1.0 service is disabled by default in Oracle ILOM 3.2.9. Support for the TLS v1.0 service is removed in Oracle ILOM as of firmware version 4.0.0.
  - TLS v1.1 service is disabled by default in Oracle ILOM 4.0.4.

- TLS v1.2 service is enabled by default in Oracle ILOM 3.2.8 and later.

Note - If the managed device is running an older Oracle ILOM firmware version that supports the configuration of SSL and weak cipher encryption properties, disable these properties and enable the TLS v1.2 encryption property to ensure secure HTTPS data transmissions.

To view or modify the web server security properties in Oracle ILOM, refer to the following web-based instructions.

1. **In the Oracle ILOM web interface, click ILOM Administration -> Management Access -> Web Server.**

2. **In the Web Server page, view or modify the web security properties as required.**

   For further details, click the **More details...** link located at the top of the Management Access -> Web Server page.

3. **Click Save to apply the changes.**

Related Information

- Web Server Configuration Properties, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Web Server Configuration Properties, *Oracle ILOM 3.1 Configuration and Maintenance Guide*

▼ Set a Timeout Interval for Inactive Web Sessions

The Oracle ILOM web session timeout intervals provide security for web access users who forget to log out. The web session time-out intervals determine how many minutes can lapse until an inactive HTTP or HTTPS web session is automatically logged out. This feature reduces the risk of an unauthorized user finding an unattended computer with an established authenticated web session to Oracle ILOM.

To view or modify the web session time-out intervals set for HTTP and HTTPS sessions, see the following web-based instructions.

Before You Begin

- The default web session time-out interval set for HTTP and HTTPS connections is 15 minutes.

Note - Lowering the session time-out might cause users to have to re-enter his or her user name and password more often, as sessions expire. However, lowering the session time-out will shorten the amount of time during which unattended authenticated web sessions remain active.

- Admin (a) role is required to modify the web server properties
- The HTTP and HTTPS session time-out interval properties are only configurable in Oracle ILOM for server SPs running firmware release 3.0.4 or later.

1. **Navigate to the Web Server page.**

   For instance, in the:

   - **3.0.x web interface, click Configuration -> System Management Access -> Web Server.**
   - **3.1 and later web interface, click ILOM Administration -> Management Access -> Web Server.**

2. **In the Web Server page, perform the following:**

   a. **Navigate to the HTTP or HTTP Session Timeout property.**

   b. **Enter a number between 1-720 minutes to specify how many minutes can lapse until an inactive web session is automatically logged out.**

   c. **Click Save to apply the changes.**

Related Information

- "Web Server Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

Configure the CLI for Increased Security

Refer to following topics for how to best configure the Oracle ILOM command-line interface (CLI) for Increased security.

- "Management of SSH Server State and Weak Ciphers " on page 52

- “Set a Timeout Interval for Inactive CLI Sessions” on page 52
- “Use Server Side Keys to Encrypt SSH Connections” on page 54
- “Append SSH Keys to User Accounts for Automated CLI Authentication” on page 55

You can configure the CLI management properties in Oracle ILOM by using the command-line interface (CLI) or web interface. The procedures in this section provide web-based navigation instructions for all Oracle ILOM firmware releases. For CLI instructions, or for additional details about configuration properties, refer to the appropriate documentation listed in the Related Information section that follows each procedure.

▼ Management of SSH Server State and Weak Ciphers

The Weak Ciphers property for SSH Management Access was first introduced in Oracle ILOM as of firmware version 3.2.5. The Weak Ciphers property was later removed in Oracle ILOM as of firmware version 3.2.6, as well as later versions of firmware versions 3.2.5.x. For systems still operating Oracle ILOM firmware supporting the Weak Ciphers property, the Weak Ciphers property should be disabled to increase security. To modify the SSH management access properties, see the following web-based instructions.

1. **In the Oracle ILOM web Interface, click ILOM Administration -> Management Access -> SSH Server.**

2. **In the SSH Server page, click the** *More Details...* **link for further instructions.**

3. **Click Save to apply your changes.**

Related Information

- “SSH Server Configuration Properties” in *Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x*
- “SSH Server Configuration Properties” in *Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 4.0.x*

▼ Set a Timeout Interval for Inactive CLI Sessions

The Oracle ILOM CLI, which is accessed by connecting to Oracle ILOM over the Secure Shell (SSH) protocol or by using a serial connection, supports a configurable session time-out interval for closing inactive CLI sessions. When configured, this feature reduces the risk of an unauthorized user finding an unattended computer with an authenticated CLI session to Oracle ILOM.

For Increased security, you should configure a CLI session time-out interval in any environment where the Oracle ILOM CLI is used on a shared console. Ideally, you should set the CLI session time-out interval to 15 minutes or less.

To view or modify the time-out interval property set for inactive Oracle ILOM CLI sessions, see the following web-based instructions.

Before You Begin

- Admin (a) role is required to modify the CLI properties.
- The default CLI session time-out interval set for SSH connections is disabled and set to 0 (zero) minutes.

Note - When the CLI time-out interval is set to 0 (zero), Oracle ILOM will not close the inactive CLI sessions regardless of the time a session remains idle.

- The CLI session time-out interval property is only configurable in Oracle ILOM for server SPs running firmware release 3.0.4 or later.

1. **Navigate to the CLI page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click Configuration -> System Management Access -> CLI.**
   - **3.1 and later web interface, click ILOM Administration -> Management Access -> CLI.**

2. **In the CLI page, set a CLI session time-out interval by performing the following.**

   a. **Select the Enable check box.**

   b. **Enter in a number between 1-1440 minutes to specify how many minutes can lapse until an inactive command-line session is automatically logged out.**

   c. **Click Save to apply the changes.**

Related Information

- "CLI Session Timeout and Custom Prompt Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

▼ Use Server Side Keys to Encrypt SSH Connections

Oracle ILOM provides a Secure Shell (SSH) server capability, allowing remote clients to securely connect and manage Oracle ILOM through a command-line interface. The SSH protocol uses server-side keys to encrypt the management channel and secure all communication. SSH clients also use these keys to verify the authenticity of the SSH server.

Oracle ILOM generates a set of unique SSH keys on the first boot of a factory default system. In the event that new server-side keys are needed, Oracle ILOM supports the ability to manually generate additional SSH server-side keys.

To view or manually generate SSH server-side encryption keys, see the following web-based instructions.

Before You Begin

- The Admin (a) is required to modify the SSH server properties.

1. **Navigate to the SSH Server page in the Oracle ILOM web Interface.**

   For instance, in the:

   - **3.0.x web interface, click System Management -> SSH Server.**

   - **3.1 and later web interface, click ILOM Administration -> Management Access-> SSH Server.**

2. **In the SSH Server page, review the generated RSA and DSA Key information, or perform the following:**

   a. **Click Generate RSA Key to generate a new key.**

   b. **Click Generate DSA Key to generate a new key.**

Related Information

- "SSH Server Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

▼ Append SSH Keys to User Accounts for Automated CLI Authentication

Custom generated SSH key pairs (DSA or RSA) can be used for individual user accounts, with the public key being uploaded to Oracle ILOM. This is beneficial when using scripts that execute without manual intervention and do not include embedded clear text passwords. Users can write scripts that automatically or regularly execute service processor commands over a network-based SSH connection from a remote system.

To upload and append an Oracle ILOM account with a generated public SSH key, see the following web-based instructions.

Before You Begin

- Generate the private and public SSH keys using an SSH connectivity tool, like ssh-keygen, and then store the generated SSH key files on a remote SSH system.
- The User Management (u) role is required to configure user account properties for other users. Any user can modify their user account password.
- The User Management (u) role is required to append SSH public keys to other user accounts.
- The Read Only (o) role is required to append an SSH public key to your own user account.

1. **Navigate to the User Account page in the Oracle ILOM web interface.**

   For instance, in the:

   - **3.0.x web interface, click User Management -> User Accounts.**
   - **3.1 and later web interface, click ILOM Administration -> User Management -> User Accounts.**

2. **In the User Account page, perform the following:**

   Note - For further configuration details, click the **More details...** link located at the top of the User Management -> User Accounts page.

   a. **Scroll-down to the SSH Keys section and click Add.**

   Note - The Increased SSH key size for RSA is 8192 bits. The SSH key size for DSA must be 1024 bits.

   b. **Select a user account from the User list.**

c. **Select a transfer method from the list, and then specify the required transfer method properties for uploading the public SSH key.**

3. **Click Load to upload the public SSH key and append it to the selected user account.**

Related Information

- "CLI Authentication Using Local User SSH Key" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

Configure SNMP Management Access for Increased Security

Note - SNMP set operations and writeable SNMP MIBs are not supported in Oracle ILOM as of firmware version 4.0.x.

SNMP is a standard protocol used to monitor or manage a system. Oracle ILOM provides an SNMP solution for both monitoring and management, but it must be configured prior to use. It is important to understand the security implications of the various SNMP user-configurable options before configuring this service. For further details, see the following information:

- "Use SNMPv3 Encryption and User Authentication" on page 56
- "Sun SNMP MIBs Supporting Configurable Objects" on page 58

▼ Use SNMPv3 Encryption and User Authentication

Note - SNMP set operations and writeable SNMP MIBs are not supported in Oracle ILOM as of firmware version 4.0.x.

SNMPv1 and SNMPv2c provide no encryption and use community strings as a form of authentication. Community strings are sent in clear text over the network and are usually shared across a group of individuals, rather than being private to an individual user. SNMPv3, conversely, uses encryption to provide a secure channel as well as individual user names and passwords. SNMPv3 user passwords are localized so that they can be stored securely on management stations.

SNMPv1, SNMPv2c, and SNMPv3 are all supported by Oracle ILOM and can be enabled or disabled separately. In addition, "sets" can be enabled or disabled to provide an additional layer of security. This configurable option determines whether the SNMP service will allow configurable SNMP MIB properties to be set. Disabling sets effectively makes the SNMP service useful for monitoring only.

By default, SNMPv1 and SNMPv2c are disabled. SNMPv3 is enabled by default, but requires creating one or more SNMP users prior to use. There are no preconfigured SNMPv3 users.

To configure SNMP management in Oracle ILOM, see the following web-based instructions.

Before You Begin

- For Increased SNMP security, use SNMPv1 and SNMPv2c only for monitoring and do not enable “sets” when these less secure protocols are enabled.
- SNMP sets should only be enabled for SNMPv3 management. The SNMP Set property is disabled by default.

Note - As of Oracle ILOM firmware version 4.0.x, SNMP set operations and writeable SNMP MIBs are not supported.

- SNMPv3 sets require the configuration of SNMPv3 user accounts. Preconfigured SNMPv3 user accounts are not provided.
- The SNMP service State property is enabled by default.
- Admin role (a) privileges are required to modify the SNMP properties.
- User management (u) privileges are required to add or modify SNMPv3 user accounts.

1. **Navigate to the SNMP page in the Oracle ILOM web interface.**

   For instance:

   - **3.0.x web interface, click System Management Access -> SNMP.**
   - **3.1 and later web interface, click ILOM Administration -> Management Access -> SNMP.**

2. **In the SNMP page, view or modify the SNMP properties, and then click Save to apply the changes.**

   For further instructions, see the documentation listed in the Related Information section of this procedure. For users running firmware version 3.2 or later, click the `More details` link in the SNMP page for additional information.

Related Information

- "SNMP Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*
- "Configuring SNMP Settings in Oracle ILOM" in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*
- "Configuring SNMP Settings in Oracle ILOM" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x*

Sun SNMP MIBs Supporting Configurable Objects

Note - SNMP set operations and writeable SNMP MIBs are not supported in Oracle ILOM as of firmware version 4.0.x.

Oracle's Sun MIBs that support configurable objects and where "sets" are applicable are as follows:

- `SUN-HW-CTRL-MIB` – This MIB is used to configure hardware policies, such as power management policies.
- `SUN-ILOM-CONTROL-MIB` – This MIB is used to configure Oracle ILOM features, such as creating users and configuring services.

Note - You can set a MIB object when: 1) the MIB object supports modification; 2) the `MAX-ACCESS` element for the MIB object is set to `read-write`; and 3) the user attempting to perform the set is authorized to do so.

Configure IPMI Management Access for Increased Security

Refer to following topics for how to best configure the Oracle ILOM IPMI management access for increased security.

- "Use IPMI TLS Service for Enhanced Authentication and Packet Encryption" on page 59
- "Oracle ILOM IPMI Security Guidelines" on page 60
- "IPMI 2.0 Authentication Cypher Suite Support" on page 61

▼ Use IPMI TLS Service for Enhanced Authentication and Packet Encryption

Although Oracle ILOM supports both IPMI v1.5 and v2.0 for remote management, system administrators should always use the IPMI TLS service and the `- I orcltls` interface to securely manage Oracle servers. For further information about how to securely configure and establish an IMPI TLS management session with Oracle ILOM, see the following information.

Before You Begin

- For enhanced security, use only the TLS service and the `- I orcltls` interface for all IPMI management sessions. For additional IPMI security guidelines, see "Oracle ILOM IPMI Security Guidelines" on page 60.

Note - The TLS service and interface from Oracle is supported in Oracle ILOM as of firmware version 3.2.8.

- The Admin (a) role is required to modify IPMI properties in Oracle ILOM.
- To use the TLS IPMItool interface, IPMItool users must use IPMItool v1.8.15.0 or later, which is available for download from Oracle Hardware Management Pack (version v2.4 for Linux or version 4.0 for Solaris).

Note - Before using IPMItool, you need to set up users with the appropriate roles and privileges (such as Administrator or Operator) for the management functions you want to perform. For more information about setting up user accounts, see "Setting Up and Maintaining User Accounts" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*.

To implement a more secure IPMI TLS management session with Oracle ILOM, perform these steps:

1. **Disable the IPMI v2.0 Session Property in Oracle ILOM.**

   For instance:

   a. **In the Oracle ILOM web interface: click ILOM Administration-> Management Access -> IPMI.**

   b. **In the IPMI page, disable the IPMI v2.0 Sessions check box, and then click Save.**

For Oracle ILOM CLI instructions, see "Set the IPMI State and Session Properties (CLI)" in *Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x*

2. **Download the TLS version of the IPMItool from the Oracle Hardware Management Pack (version 2.4 for Linux or version 4.0 for Oracle Solaris).**

   For further download instructions, see "IPMI TLS Service and Interface" in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*.

3. **From the Oracle ILOM CLI, access the TLS IPMItool interface by typing:**

   ```
   ipmitool -I orcltls
   ```

   Note that in cases where the `-I` option is not specified, the IPMItool utility will negotiate to the most secure interface available (in the following order):

   - TLS 1.2 (`orcltls` interface)
   - TLS 1.1 (`orcltls` interface)
   - TLS 1.0 (`orcltls` interface)

   For additional information about how to use the `orcltls` interface to manage and configure IPMI-enabled devices, refer to following information:

   - "IPMI TLS Service and Interface" in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*.
   - "Performing System Management Tasks (IPMItool)" in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*
   - "IPMItool Options and Command Summary" in *Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 4.0.x*

Related Information

- "Oracle ILOM IPMI Security Guidelines" on page 60
- "IPMI 2.0 Authentication Cypher Suite Support" on page 61

Oracle ILOM IPMI Security Guidelines

To ensure that established IPMI system management sessions are secure and not vulnerable to cyber attacks, system administrators should:

- Never establish IPMI remote management sessions using IPMI v2.0 (`-I lanplus` IPMItool interface) or IPMI version 1.5 (`-I lan` IPMItool interface). You should explicitly use the IPMI TLS service and `orcltls` interface as of Oracle ILOM firmware version 3.2.8 and later.

Note - The RAKP protocol support in the IPMI 2.0 specification requires sending a password hash to the client, which makes it easier for remote attackers to obtain access via a brute-force attack. For additional details about this vulnerability, see the published vulnerability summaries for CVE 2013-4037 and CVE 2013-4786 on the National Vulnerability Database web site.

Note - The Oracle ILOM IPMI Session property for version 1.5 is disabled by default as of Oracle ILOM firmware 3.2.4. The Oracle ILOM IPMI Session property for v2.0 is enabled by default. For additional information about IPMI v2.0 support in Oracle ILOM, see "Deprecation Notice for IPMI 2.0 Management Service" in *Oracle ILOM Feature Updates and Release Notes Firmware Release 3.2.x*,

- Change your IPMI password on a regular basis. Ensure the lifecyle of Oracle ILOM user accounts are managed appropriately.

  For further details, see "Securing Oracle ILOM User Access" on page 27.
- Restrict network access from the outside world. Use the dedicated Ethernet management channel to communicate with Oracle ILOM.

  For further details, see "Securing the Physical Management Connection" on page 17.
- Work with your IT Security Officer to build a set of best practices and policies around server management and IPMI security.

IPMI 2.0 Authentication Cypher Suite Support

Note - For IPMI v2.0 configuration planning purposes, see "Deprecation Notice for IPMI 2.0 Management Service" in *Oracle ILOM Feature Updates and Release Notes Firmware Release 3.2.x*

The authentication, confidentiality, and integrity checks in IPMI version 2.0 are supported through cipher suites. These cipher suites use the RMCP+ Authenticated Key-Exchange Protocol as described in the IPMI 2.0 specification.

Oracle ILOM supports the following cipher suite key algorithms for establishing secure IPMI 2.0 sessions between the client and the server.

- **Cipher Suite 2** – Cipher suite 2 uses both authentication and integrity algorithms.
- **Cipher Suite 3** – Cipher suite 3 uses all three algorithms for authentication, confidentiality, and integrity.

Note - To ensure all IPMI 2.0 traffic is encrypted, Oracle ILOM does not implement support for IPMI 2.0 Cipher Type 0 (unencrypted mode of operation).

Configure WS-Management Access for Increased Security

Note - As of firmware release 3.1.2, the WS-MAN API has been deprecated in Oracle ILOM. Oracle ILOM versions 3.1.2 and earlier will continue to support the WS-MAN API.

As of firmware release 3.0.8 to firmware release 3.1.2, Oracle ILOM provides a standard, web-services interface for monitoring the health of the server and providing inventory information using a protocol called Ws-Management (Ws-Man).

The Oracle ILOM Ws-Man interface also allows for peer control of the host and for resetting the Oracle ILOM SP itself. Ws-Man is a Simple Object Access Protocol (SOAP)-based protocol, leveraging the HTTP(S) protocols. The Oracle ILOM Ws-Man interface can be used with either HTTP or HTTPS as a transport. If HTTPS is used, the channel is encrypted using an SSL certificate. For information about the security benefits of using SSL certificates, as well as the difference between self-signed versus trusted certificates, see "Improve Security by Using a Trusted SSL Certificate and Private Key" on page 42.

Use this web-services interface only if SSL certificates are being used. For Increased security, use HTTPS as the transport mechanism. For more information about configuring web server properties, see "Configure the Web Interface for Increased Security" on page 41.

Oracle ILOM Post Deployment Practices for Increasing Security

Use the following topics to decide the best Oracle ILOM deployment practices to implement after server deployment.

- "Maintaining a Secure Management Connection" on page 63
- "Using Remote KVMS Securely" on page 66
- "Post Deployment Considerations for Securing User Access" on page 69
- "Post Deployment Actions for Modifying FIPS Mode" on page 72
- "Updating to the Latest Software and Firmware" on page 75

Related Information

- "Oracle ILOM Deployment Practices for Increasing Security" on page 17
- "Checklists for Keeping Oracle ILOM Secure" on page 13

Maintaining a Secure Management Connection

Consider the following information for maintaining a secure management connection to Oracle ILOM.

- "Avoid Unauthenticated Host KCS Device Access" on page 63
- "Preferred Authenticated Host Interconnect Access" on page 64
- "Use Secure Protocols for Remote Management" on page 65

Avoid Unauthenticated Host KCS Device Access

Oracle servers supports a standard, low-speed connection between the host and Oracle ILOM called a Keyboard Controller Style (KCS) interface. This supported KCS interface is fully compliant with the Intelligent Platform Management Interface (IPMI) and likewise cannot be disabled.

While KCS device access might be a convenient way to configure Oracle ILOM from the host, this type of access can also presents security risks since any operating system user who has kernel or driver access to the physical KCS device can modify the Oracle ILOM settings without authentication. Typically, only `root` or Administrator users can access the KCS device. However, it is possible to configure most operating systems to provide wider access to the KCS device.

For instance, an operating system user with KCS access can do the following:

- Add or create Oracle ILOM users.
- Change user passwords.
- Access the Oracle ILOM CLI as an ILOM Administrator.
- Access logs and hardware information.

Typically, the device is called `/dev/kcs0` or `/dev/bmc` on Linux or Oracle Solaris and `ipmidrv.sys` or `imbdrv.sys` on Microsoft Windows. Access to this device, also referred to as a Baseboard Management Controller (BMC) driver or an IPMI driver, must be carefully controlled using the appropriate access control mechanisms that are part of the host operating system.

As an alternative to using the host IPMI KCS device to configure Oracle ILOM settings, consider using the Oracle ILOM Interconnect interface. For further details, see "Preferred Authenticated Host Interconnect Access" on page 64.

For additional information on how to control or protect access to hardware devices such as the KCS device, see the documentation provided with the host operating system.

Preferred Authenticated Host Interconnect Access

As a faster alternative to the KCS interface, clients on the host operating system can communicate with Oracle ILOM over an internal high-speed interconnect. The interconnect is implemented by an internal Ethernet-over-USB connection, running an IP stack. Oracle ILOM is given an internal, non-routable IP address that a client on the host can use to connect to it.

Unlike the KCS interface, which relies on protected access to a hardware device, the LAN interconnect is available to all operating system users by default. Therefore, connecting to Oracle ILOM over the LAN interconnect requires authentication, just as if the connection were coming over the network to the Oracle ILOM management port.

In addition, all services or protocols exposed on the management network are made available over the LAN interconnect to the host. It is possible to use a web browser on the host to access the Oracle ILOM web interface or use a Secure Shell client to connect to the Oracle ILOM command-line interface. In all cases, a valid user name and password must be provided to use the LAN interconnect.

The LAN interconnect is disabled by default. When it is disabled, there is no Ethernet device visible to the host operating system and the channel does not exist. Oracle Hardware Management Pack helps provision and configure the LAN interconnect.

For information about managing Oracle ILOM through a secure dedicated host interconnect connection, see one of the following:

- For firmware releases 3.2 or later, see Dedicated Interconnect SP Management Connection in the *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2x)*
- For firmware releases 3.1.x, see Dedicated Interconnect SP Management Connection in the *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- For firmware release 3.0.12 to 3.0.16, see Configuring Local Host Interconnect in the *Oracle ILOM 3.0 Web Procedures Guide.*

Use Secure Protocols for Remote Management

Oracle ILOM supports a number of different remote management protocols. In some cases, support is provided for both encrypted and non-encrypted versions of the same protocol. For security reasons, you should always use, if possible, the most secure protocol available. For a list of supported encrypted and non-encrypted protocols, see the following table.

TABLE 9 Supported Secure Protocols

Category	Secure/Encrypted	Non-encrypted
Web browser access	HTTPS	HTTP
Command-line access	SSH	None supported
IPMI access	TLS (preferred service for IPMI, see “Configure IPMI Management Access for Increased Security” on page 58) IPMI v2.0	IPMI v1.5
Protocol access	SNMPv3	SNMPv1/v2c

Establish a Secure Trusted Network Management Connection

All Oracle servers with Oracle ILOM have a dedicated management port used for connecting to Oracle ILOM over a network. Using the dedicated management port provides a private and secure network for management. Some systems also support sideband management that allows both the host and Oracle ILOM to be accessible on the standard server data ports. Using sideband management simplifies cable management and network configuration by preventing the need for two separate network connections. However, it also means that Oracle ILOM traffic could potentially be sent over an untrusted network if the dedicated or sideband management port is not connected to a trusted network.

To maintain the most reliable and secure environment for Oracle ILOM, the dedicated network management port or the sideband management port on the server must always be connected to an internal trusted network or dedicated secure management/private network.

Establish a Secure Local Serial Management Connection

You can locally connect a terminal server or a dump terminal to Oracle ILOM through the physical serial management port that is located on the server. To maintain a secure local management connection to Oracle ILOM, avoid connecting a terminal device to the local serial management port if that device is also connected to an internal or private network.

Using Remote KVMS Securely

Oracle ILOM provides the ability to remotely redirect the keyboard, video, and mouse of the host server to a remote client, as well as to mount remote storage. These features are collectively called Remote KVMS. Remote KVMS allows you to see the graphical console of the host operating system on the server by running Java applications called Oracle ILOM Remote Console, Remote Console Plus, and CLI Storage Redirection on a client machine.

To ensure that remote KVMS and serial text-based sessions are securely launched from Oracle ILOM, consider the following:

- “KVMS Remote Communication and Encryption” on page 67
- “Protect Against Remote KVMS Shared Access” on page 67

- “Protect Against Host Serial Console Shared Access” on page 68

KVMS Remote Communication and Encryption

The Oracle ILOM Remote System Console, Remote System Console Plus, and the CLI Storage Redirection applications use a series of network protocols to remotely communicate with Oracle ILOM. Using these Java applications, you can control the host keyboard and mouse and mount a local storage device (such as a CD or DVD drive) on the remote server.

The following table describes, in more detail, the way in which Remote KVMS information is transmitted over the network.

TABLE 10 KVMS Features and Encryption

KVMS Feature	Encrypted or Not Encrypted	Description
Mouse Redirection	Encrypted	The coordinates of your mouse are securely sent over the network to Oracle ILOM.
Keyboard redirection	Encrypted	Any characters that you type on the client machine are transmitted to Oracle ILOM using an encrypted protocol.
Video redirection	Encrypted	The video data is transmitted using an encrypted protocol between the Java client and Oracle ILOM.
Storage Redirection	Not Encrypted	Data read and written to a storage device is transmitted over the network to Oracle ILOM without encryption.

For a list of network ports enabled by remote KVMS, see Table 4, “Services and Ports Enabled by Default,” on page 22.

Protect Against Remote KVMS Shared Access

A remote KVMS video console redirects what you would see if you were looking at a physical monitor connected to that server. While it is possible to have multiple remote clients with KVMS sessions to Oracle ILOM, each session will display the exact same video since there is typically only one video output for a single server.

Likewise, anything that you type on the screen from one Remote KVMS session will be visible to other KVMS users connected to the same machine. Most importantly, if one user logs in to the host operating system inside of the Oracle ILOM Remote Console, Remote Console Plus, or CLI Storage Redirection application as a privileged user, all other KVMS users will be able to share that authenticated session. Therefore, it is important to understand that the Remote KVMS feature allows for shared connections.

To protect against authenticated operating system sessions that are left idle after terminating a remote KVMS redirection session, you should:

- Configure Oracle ILOM to automatically lock the host operating system upon terminating a remote KVMS redirection session.

  For instructions, see "Lock Host Access Upon Exiting a KVMS Session" on page 36.
- Set a time-out interval in the host operating system to automatically close unattended authenticated user sessions.

  For instructions, refer to the user documentation for your host operating system.

If you are an Oracle ILOM Remote System Console Plus user and need to limit the number of viewable KVMS sessions launched from Oracle ILOM, see "Limit Viewable KVMS Sessions for Remote System Console Plus (3.2.4 or later)" on page 37.

Protect Against Host Serial Console Shared Access

The host console for most operating systems is also available using a text-based, serial console. This console is available by running the `start /HOST/console` command at the command-line of the Oracle ILOM CLI. Similar to the graphical console, there is only a single serial console available to all Oracle ILOM users. Therefore, it is considered a shared resource. If one user logs in to the host operating system from the serial console and then terminates the console redirection without logging out, a second user of the serial console could access the previously authenticated operating system session.

Oracle ILOM sends a Data Transfer Request (DTR) signal to the host operating system when a console redirection session is terminated. Many operating systems automatically log out a user when this signal is received. However, not all operating systems have support for this feature:

- Oracle Linux 5 has DTR signal support that works by default.
- Oracle Linux 6 has DTR support, but it must be enabled manually.
- Oracle Solaris has no support for the DTR signal. To reduce security risk, users can configure a session time-out in the host operating system.

For guidelines for protecting against authenticated operating system sessions that are left idle after terminating a host serial redirection session, see the following:

- Determine if the DTR signal feature in the host operating system is supported, and if it is, ensure that this feature is enabled by default.

For information about the DTR signal, refer to the user documentation for your host operating system.

- Configure a session time-out interval in the host operating system.

  For information about how to set a session time-out interval in the host operating system, refer to the user documentation for your host operating system.
- Implement a security policy to ensure that users never leave a remote serial host console unattended. Users should always logged out of all remote host console sessions when sessions are not in use.

Post Deployment Considerations for Securing User Access

To ensure secure user access is maintained, consider the following:

- "Enforce Password Management" on page 69
- "Physical Security Presence for Resetting `root` Account Default Password" on page 70
- "Monitor Audit Events to Find Unauthorized Access" on page 72

Enforce Password Management

Change all Oracle ILOM passwords on a regular basis. This prevents malicious activity and ensures that passwords remain in accordance with current password policies.

Typically, users change their own password, however, system administrators with user management privileges can modify passwords associated with other user accounts.

To change the password associated with an Oracle ILOM user account, see the following web-based instructions.

Note - For CLI instructions or other details about user management configuration properties, see the documentation listed in the Related Information section that appears in the following procedure.

▼ Modify Local User Account Password

Before You Begin

- Review the "Security Guidelines for Managing User Accounts and Passwords" on page 29.

- The User Management (u) role is required to modify passwords or privileges that are associated with other user accounts.
- The Operator (o) role permits users to modify the password for their own account.

1. **Navigate to the User Account page in the Oracle ILOM web interface.**
   For instance, in the:
   - **3.0.x web interface, click User Management -> User Accounts.**
   - **3.1 and later web interface, click User Management -> User Accounts.**
2. **In the User Account page, click Edit for the account you want to modify.**
   An Edit: User Name dialog appears.
3. **In the Edit: User Name dialog, perform the following:**
   - **Enter a unique password in the New Password text box, then re-enter the same password in the Confirm New Password text box.**
   - **Click Save to apply the change.**

Related Information

- "Set Password Policy Restrictions for All Local Users (3.2.5 and later)" on page 32
- Configuring a Local User Account, *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Configuring a Local User Account, Oracle ILOM 3.1 *Configuration and Maintenance Guide*
- Modify a User Account, *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Modify a User Account, *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Physical Security Presence for Resetting `root` Account Default Password

In the event that the `root` user password for Oracle ILOM is lost, it can be reset. To reset the `root` password, connect to Oracle ILOM through the serial port. While in most cases connection to the Oracle ILOM serial port requires physical access to the system, the serial console can be connected to a terminal server. The terminal server effectively gives network access to the physical serial port.

To prevent being able to reset the `root` password over the network when a terminal server is used, there is a physical presence check feature for most servers. This requires pushing a button on the server as a means of proving physical access to the server. For increased security, ensure the presence check feature is enabled whenever the Oracle ILOM serial port is connected to a terminal server.

To view or modify the physical presence check feature, see the following web-based instructions.

Note - For CLI instructions or other details about the `root` account properties, see the documentation listed in the Related Information section that appears in the following procedure.

▼ Set Physical Presence Check

Before You Begin

- The Physical Presence Check mode in Oracle ILOM is enabled by default.
- Firmware version 3.1 or later is required to use the Physical Presence Check mode in Oracle ILOM.

1. **In the Oracle ILOM web interface, click ILOM Administration -> Identification**

2. **In the Identification page, navigate to the Physical Presence Check property, and then perform one of the following:**

   - **Select the Physical Presence check box to enable. When enabled, the Locator button on the physical system must be pressed in order to recover the default Oracle ILOM password.**

     -or-

   - **Clear the Physical Presence check box to disable. When disabled, the default Oracle ILOM administrator root password can be reset without pressing the Locator button on the physical system.**

3. **Click Save to apply the change.**

Related Information

- "Assigning System Identification Information" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*
- "Password Recovery for Default root Account" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

Monitor Audit Events to Find Unauthorized Access

The Oracle ILOM Audit log records all logins and configuration changes. Each audit log entry notes the user and time stamp associated with the event. Audit events can be a useful tool for tracking changes, and also for determining whether there are unauthorized changes and unauthorized access to Oracle ILOM.

To view events in the Oracle ILOM Audit log, see the following web-based instructions.

Note - For CLI instructions or other details about the Audit log, see the documentation listed in the Related Information section of the following procedure.

▼ View Audit Log

Before You Begin

- The Audit log became available in Oracle ILOM as of firmware release 3.1. Prior to firmware release 3.1, the audit events were captured in the Oracle ILOM Event log.
- Admin (a) role privileges are required in Oracle ILOM to clear entries in the Audit log.

1. **In the web interface, click ILOM Administration -> Logs -> Audit.**

2. **In the Audit log page, use the controls to filter the log entries, or to clear events in the log.**

   For users running firmware version 3.2. or later, click the `More details` link on the Audit page for additional information.

Related Information

- "Managing Oracle ILOM Log Entries" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 4.0.x*

Post Deployment Actions for Modifying FIPS Mode

As of firmware release 3.2.4, Oracle ILOM provides a configurable property for FIPS level 1 compliance. By default, this property is shipped disabled. Upon modifying the operational status of FIPS compliance in Oracle ILOM, all user-defined configurations properties are reset to their factory default settings. To avoid the loss of user-defined configuration settings in Oracle ILOM, FIPS compliance should be modified prior to configuring any other Oracle ILOM setting. In the event FIPS compliance must be modified post deployment of Oracle ILOM's configuration, see the following instructions to avoid the loss of user-defined settings.

Note - Oracle uses cryptographic algorithms in compliance with the FIPS 140-2 security standards for protecting system sensitive or valuable data.

▼ Modify FIPS Mode Post Deployment

Use this procedure if you need to modify the FIPS mode operational state after performing a firmware update or specifying user-defined configuration properties in Oracle ILOM.

Note - FIPS compliance mode in Oracle ILOM is represented by a State and Status property. The State property represents the configured mode in Oracle ILOM and the Status property represents the operational mode in Oracle ILOM. When the FIPS State property is changed, the change does not affect the operational mode (FIPS Status property) until the next Oracle ILOM reboot.

Before You Begin

- The configurable property for FIPS level 1 compliance is available in Oracle ILOM as of firmware 3.2.4 or later. Prior to firmware release 3.2.4, Oracle ILOM does not provide a configurable property for FIPS level 1 compliance.
- When FIPS is enabled (configured and operational) some features in Oracle ILOM are not supported. For a list of unsupported features when FIPS is enabled, see “Unsupported Features When FIPS Mode Is Enabled” on page 20.
- The Admin (a) role is required to modify the FIPS State property on the Management Access > FIPS page.
- To Restore the Oracle ILOM configuration, the following user privileges must be assigned:
    - Administrator (administrator) profile or

      -or-
    - Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o)

To modify the FIPS mode after updating the Oracle ILOM firmware, follow these steps:

1. **In the Oracle ILOM web interface back up the Oracle ILOM configuration.**

   For instance:

a. **Click ILOM Administration -> Configuration Management -> Backup/Restore.**

b. **In the Backup/Restore page, click the More details... link for further instructions.**

Note - To simplify the reconnection to Oracle ILOM after the firmware update, you should enable the firmware update options for Preserve the Configuration.

Note - If you perform Step 2 before you perform Step 1, you will need to edit the XML backed-up configuration file and remove the FIPS setting. Otherwise, you will have an inconsistent configuration between the backed-up Oracle ILOM XML file and the operational FIPS mode state running on the server, which is not allowed.

---

2. **If a firmware update is required, perform the following steps:**

   a. **Click ILOM Administration -> Maintenance -> Firmware Update.**

   b. **In the Firmware Update page, click the More details... link for further instructions.**

3. **Modify the FIPS compliance mode in Oracle ILOM as follows:**

   a. **Click ILOM Administration -> Management Access -> FIPS.**

   b. **In the FIPS page, click the `More details` link for instructions on how to:**

      - **Modify the FIPS State configuration.**
      - **Update the FIPS operational status on system by resetting the SP.**

4. **Restore the backed-up Oracle ILOM Configuration as follows:**

   a. **Click ILOM Administration -> Configuration Management -> Backup/Restore.**

   b. **In the Backup/Restore page, click the `More details` link for further instructions.**

Related Information

- "Choosing Whether to Configure FIPS Mode At Deployment" on page 18

- "Unsupported Features When FIPS Mode Is Enabled" on page 20
- "Operating Oracle ILOM in FIPS Compliance Mode" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 4.0.x*

Updating to the Latest Software and Firmware

Keep your software and firmware versions current on your server.

- Check regularly for updates posted on My Oracle Support.
- Take advantage of bug fixes and enhancements by always installing the latest released version of the software or firmware available for your server.
- Install any necessary security patches required for all installed software.

To update the Oracle ILOM firmware on your server, see the following instructions.

▼ Update Oracle ILOM Firmware

Before You Begin

- Admin (a) role in Oracle ILOM is required to update the Oracle ILOM firmware.
- Notify all Oracle ILOM users of the scheduled firmware update and ask them to close all client sessions until the firmware update is complete.
- The firmware update process takes several minutes to complete, during this time no other Oracle ILOM tasks should be performed.

1. **Download the latest software update available for your server from the My Oracle Support (MOS) web site.**

   If necessary, refer to the documentation provided with your server for instructions for obtaining software updates from MOS.

   Note - The latest Oracle ILOM firmware version available for your server is included in the latest software patch that is posted on MOS for your server.

   ---

2. **Place the firmware image on a local or network shared drive.**

3. **Navigate to the Firmware Update page in the web interface.**

   For instance:

- **In the 3.0.x web interface, click Maintenance -> Firmware.**
- **In the 3.1 or later web interface, click ILOM Administration -> Maintenance -> Firmware Upgrade.**

4. **In the Firmware Upgrade page, click Enter Firmware Upgrade mode, and then follow the prompts.**

   For users running Oracle ILOM firmware 3.2 or later, click the `More details` link on the Firmware Upgrade page.