ORACLE® ACME PACKET OCSDM FAMILY

Security Guide

OCSDM 7.4

April 2014

ORACLE®

Contents

Acronyms and Definitions

Acronym	
AAA	Authentication, Authorization and Accounting
ACP	Acme Control Protocol
CPU	Critical Patch Updates
OCSDM	Oracle Communications Session Delivery Manager
SBC	Session Border Controller
SNMP	Simple Network Management Protocol
SSO	Single Sign On
XSS	Cross Site Scripting
CSRF	Cross-site Request Forgery
SFTP	Secured File Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
LDAPS	Lightweight Directory Access Protocol over SSL
SSH	Secure Shell
DB	Database
RNG	Random Number Generator
TLS	Transport Layer Security

OCSDM Security related Documentation

- Oracle® Communications Session Delivery Manager Installation Guide Release 7.4
- Oracle® Communications Session Delivery Manager Core Functionality Guide Release 7.4
- Oracle® Communications Session Delivery Manager Administration Guide Release 7.4
- Oracle® Communications Route Manager Guide Release 7.4
- Oracle® Acme Packet SBC Family Security Guide
- Oracle® Communications S-CZ7.1.2 ACLI Configuration Guide
- Oracle® Communications Session Delivery Manager High Availability Guide 7.4
- Oracle® Communications Session Element Manager Web Services SOAP/XML Provisioning API Guide 7.4
- M&A Security checklist for SDM.

Oracle documentation is available from Oracle Technology Network: http://docs.oracle.com

Chapter 1: OCSDM Security Overview

The Oracle Communications Session Delivery Management "OCSDM" family provides element management applications used to manage, monitor and configure Oracle Communications products (e.g., SBC, TSM, SR, MSG, USM, CSM). OCSDM includes:

1. Oracle Communications Session Element Manager
2. Oracle Communications Session Report Manager
3. Oracle Communications Session Route Manager

OCSDM provides web based applications with a user interface that runs in a browser or programmatically via a SOAP API. As part of providing user access via the web the application products have been designed upfront with security in mind and careful attention to reviewing new security requirements and consistent validation of user interactions.

Basic Security Considerations

The following principles are fundamental to using any application securely:

Keep software up to date. One of the principles of good security practice is to keep all software versions up to date. Oracle maintains multiple OCSDM streams or versions that are updated with applicable security patches. Oracle constantly reviews the latest security vulnerabilities and if required applies the necessary critical patch updates and updates the release notes accordingly. Throughout this document, a minimum software release of at least OCSDM 7.4 is assumed so the guide can be applicable to multiple releases.

Limit privileges as much as possible. SDM comes with the following default user groups: administrators, LIadministrators, provisioners, and monitors. The users belonging to the administrators group are the only ones who have a full set of permissions. The system provides authorization via role-based access control with dedicated user accounts that have pre-assigned privilege levels. These are discussed further in the section on management interfaces. The system offers local and remote authentication mechanisms and a role-based security policy.

Monitor system activity. Monitoring system activity is critical to determine if someone is attempting to abuse system services and to detect if there are performance or availability issues. Useful monitoring information can be acquired through Audit Logs, System Logs, SNMP and RADIUS accounting. Features such as inactivity timer will also help this cause.

Install software securely. It is always recommended that OCSDM be installed with secured measures in mind. Opting for HTTPS while installation, opting for ACP over secured TLS, securing the link between client, server and SBC are recommended.

Keep up to date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site:

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of OCSDM Security

OCSDM Specific Security Considerations

1) OCSDM products periodically upgrade third party components to keep up with security patches.

2) Oracle maintains Critical Patch Updates, Security Alerts and Third Party: http://www.oracle.com/technetwork/topics/security/alerts-086861.html which lists announcements of security fixes made in Critical Patch Update Advisories and Security Alerts, and it is updated when new Critical Patch Update Advisories And Security Alerts are released. Customer can receive notification of new announcements by email, as explained in the page.
   This page contains the following sections:

   Critical Patch Updates
   Security Alerts
   Third Party Bulletin
   Public Vulnerabilities Fixed
   Policies
   Reporting Security Vulnerabilities
   Critical Patch Updates

3) Identity management or single sign-on (SSO) technologies are supported using SAML.

4) Some of the secured Communication protocols used in the product are SFTP, HTTPS, LDAP, SSH, and ACP over TLS.

5) Account management policies create or use default database , OS, or application user accounts:
   a. Default database accounts are restricted for access to the local server only (Postgres). An OS user and group called nncentral must be created to set permissions and lock down file systems.
   b. A sudo user for TRAP Relay only.

6) No default passwords are used in the system. All passwords are obtained during system run time. All the passwords generated, stored, or transmitted are encrypted using Password Based Encryption.
7) As part of securing the file system, SDM ensures that file permissions for generated files (such as temp files, configuration files, and log files) are as restrictive as possible and doesn't have any generated files that are world readable or writeable.
8) Mechanisms to authenticate users or services accessing the system:
    a. Local authentication and authorization
    b. RADIUS and Active directory authentication.
9) Static and dynamic security testing performed on the product and the source periodically per each release.

Recommended Deployment Configurations

This section outlines the deployment possibilities for the OCSDM system.

All these products of OCSDM subscribe to a common comprehensive and granular User management scheme which is covered in the Chapter 3 of this document.

Element Management System

Element Manager is an application that enhances the core system by providing provisioning capabilities, along with fault management and performance statistics for your managed devices. Configuration Manager lets you load and provision devices. You view events, alarms, and trap summary data with Fault Manager. And Performance Manager lets you view performance statistics collected from the SBC, such as system, SNMP, IP, and environmental statistics. Another key feature of Element Manager is Dashboard Manager, which provides a dashboard summary view with at-a-glance device status and key performance indicators for your managed devices. SDM's base system also includes Device Manager, Security Manager, and Health Monitor.

Security and user management features for Element Manager are addressed in the Part 3 of this document.

Reporting Manager

Report Manager allows you to schedule and run dynamic reports on the session delivery devices in your network. Currently, the Report Manager uses BI Publisher as its reporting engine.

The Report Manager collects raw data in CSV files from designated devices. This data is aggregated into time granularities (raw, hourly, daily, weekly, monthly) and made available for running reports.

When you set collection parameters for a device or device groups, you can specify the type of data for collection. Collection groups are based on the ACLI collection groups. This data is organized into report types such as Hardware, Diameter Director Interface, and other HDR collection groups available for reporting.

Report Manager User Permissions

Report Manager subscribe to a common comprehensive and granular User management scheme which is covered in the Chapter 3 of this document.

Below is a table presenting the permissions, and a description of setting Full or None permissions.

Permission	Scenario
Report Manager	Full: Report Manager slider is present. None: Report Manager slider is not present.
Administration	Full: Administration folder and its children nodes are present. None: Administration folder is not present.
Execute reports	Full: The Reports folder is present, and users can run operational reports and save to favorites. None: The Reports folder is not present.
Scheduled	Full: The Scheduled Reports node is present under the Reports folder. None: The Scheduled Reports node is not present.

Route Manager

Route Manager lets you easily update the local route table (LRT) data on a single device or on multiple devices. With Route Manager, you can provision large LRTs across multiple SBCs and Session Routers for numeric-based routing. Route Manager lets you:

- Import a comma-separated values (CSV) file containing routing information
- Build an XML route table from the CSV contents
- Assign a list of devices to the route set
- Generate an LRT file from the route set
- Push the LRT file to all assigned devices
- Refresh the LRT data on the device using the LRT file that was pushed
- Backup, restore, and rollback route sets

Route Manager Privileges

Depending on your level of user privileges (or privileges set for the User Group you belong to), you can perform certain operations in Route Manager. The operations are:

- Configure route sets
- Configure templates
- Backup/Restore
- Device operations

Route set group privileges (also called permissions) are directly associated with the group privileges that belong to the SBC which owns the route set. For example, you might be a member of a group with full privileges to perform all route operations for Device A, but might have limited privileges to only configure templates for Device B. Each route set inherits the privileges that belong to the device which created the route set.

If you belong to a group with no privileges granted for a device, the same level of privileges would apply to the route sets associated with the device, and you would have no privileges to work with the route sets.

SIP Trunk Manager

Oracle's SIP Trunk Manager is an easy-to-use, graphical application for configuring SIP trunks. Its main purpose is to simplify the configuration of both the Service Provider and Enterprise SBCs on both ends of a SIP trunk.

SIP-based communications services are expanding to reach more subscribers in Service Provider networks. This growth has increased the number of SIP trunks needed to support the footprint of these services and their configuration is becoming much more time consuming. SIP Trunk Xpress provides centralized management of SIP trunks, allowing for automated configuration and on-going management of trunk configurations from a centralized location. SIP Trunk Xpress provides a simple mechanism to configure SIP trunk services between a SP-SBC and an E-SBC.

Trunk Manager subscribes to a common comprehensive and granular User management scheme which is covered in the Chapter 3 of this document.

Component Security

Operating System Security

See the following documents:

- Guide to the Secure Configuration of Red Hat Enterprise Linux 6
- Hardening Tips for the Red Hat Enterprise Linux 6
- Oracle Linux Security Guide for Release 6
- Tips for Hardening an Oracle Linux Server
- CentOS Wiki: OS Protection

LDAP Security

In regards to LDAP over SSH, External AAA and RADIUS and Active Directory configuration please refer to Oracle® Communications Session Delivery Manager Maintenance Release Guide Release Session Trunk Manager.

Database redundancy

Database geographic redundancy is provided via backup and restore scripts.

Please refer to Oracle® Communications Session Delivery Manager High Availability Guide 7.4 for the details.

Resiliency and High availability

Through clustering, OCSDM offers high availability and resiliency, key components of a secure deployment. When the product is deployed in a cluster, with multiple individual members, the service is not lost if one member fails.

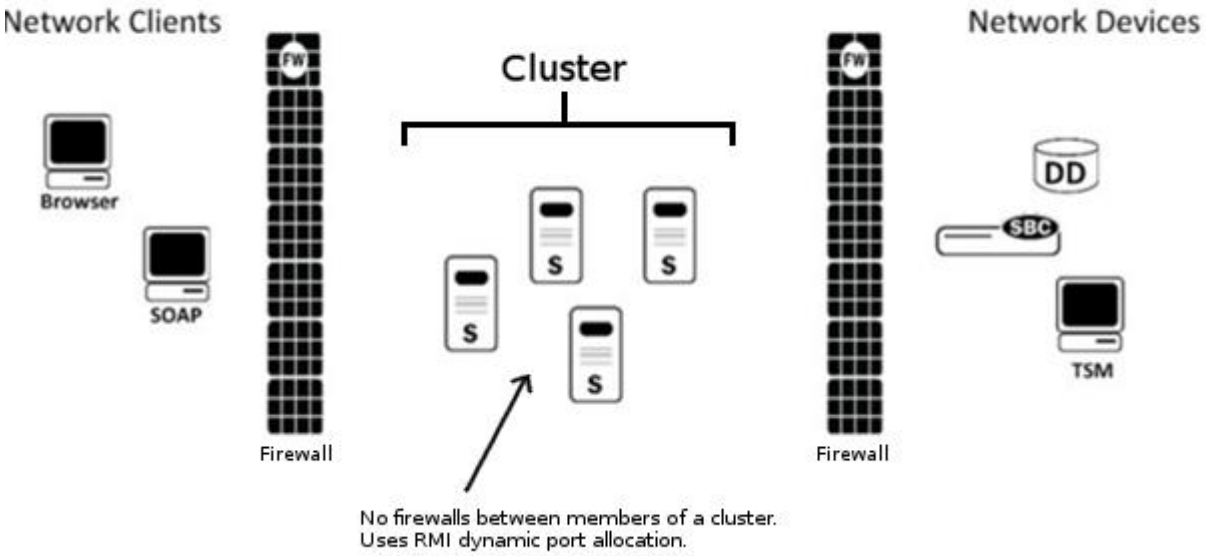
Please refer to Oracle® Communications Session Delivery Manager Installation Guide and HA Guide Release 7.4 for cluster installation for SDM.

Chapter 2: Performing a Secure Installation

Pre-Installation Configuration

Opening Ports on the Firewall before installation

When setting up Session Delivery Manager in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the SDM cluster, and a firewall between the SDM cluster and other devices (SBCs, Data Domain (DD), Terminal Server Manager (TSM)). See the following illustration.



Note: You cannot have firewalls between the servers in a cluster. If firewalls exist on either side of the Session Delivery Manager cluster, ensure the ports listed in the following table are open. If your OS system comes with a firewall, you need to apply the same criteria. You must switch off the firewall in your OS, or ensure these ports are available.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
Between Net-Net Central Cluster and Network Clients					
8443	TCP/SSL	HTTPS	N	Y	Apache port. HTTPS port for client/server communication.
8080	HTTP	HTTP	N	Y	HTTP port for client/server communication.
Between Net-Net Central Cluster and Network Devices					
161	UDP	SNMP	N	Y	SNMP read/write requests between the Net-Net Central server and the Net-Net SBC.
162	UDP	SNMP	N	Y	SNMP trap reporting from the Net-Net SBC to the Net-Net Central server.
22/21	SFTP/FTP				Used for file transfer (such as Route Manager and LRT updates).
8080	HTTP	AMI	N	Y	Used by NNC to communicate with Net-Net 9200 devices via AMI.
5060	TCP		N	Y	Used for Net-Net Central Trunk Manager (SIPTX) to communicate with SP-SBC.
3001/ 3000		ACP/ACLI			Used by Net-Net Central to communicate with all versions of Net-Net SBC except for the Net-Net 9200.
Between Net-Net Central Servers in the Cluster					
1098	TCP/SSL	RMI	N	Y	RMI Communication between host members in a cluster. Note: SSL is not supported when HTTPS is enabled.
1099	TCP/SSL	RMI Lookup	N	Y	RMI registry port. Used for the RMI communication between host members in a cluster. Note: SSL is not supported when HTTPS is enabled.
5701	TCP	Hazelcast	N		Used by Hazelcast communication for distributed data structures, peer-to-peer collective data distribution.
5801	TCP	Hazelcast	N	Y	Used by the Hazelcast management console port for the NNC distributed scheduler service.
8005	TCP	HTTP	N	Y	Tomcat shutdown port used by the shutdown script. Can be blocked on a firewall because it is local to the Net-Net Central server.
8009	TCP	Apache	N	Y	Tomcat port.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you choose between the network client and Session Delivery Manager server. If installing on a Linux system, the Linux firewall must also have either 8080 (HTTP) or port 8443 (HTTPS) open.

Note: For iptables/ipf, communication is open between Session Delivery Manager servers in a cluster if the ports listed above are open and there is no firewall deployed between the servers, as ports are assigned dynamically (Remote Method Invocation (RMI) dynamic port allocation).

Secured OCSDM Installation

HTTP installation:

OCSDM supports HTTP mode during installation. Please refer to Oracle Communications Session Delivery Manager Installation Guide 7.4 for the details.

HTTPS installation

OCSDM supports HTTPS mode during installation. HTTPS makes the communication secured over the network. Please refer to Oracle Communications Session Delivery Manager Installation Guide 7.4 for the details.

1) Enter 2 to configure HTTPS and press Enter. You are prompted about continuing.

```
Please select an option [1] 2


[ ]  1 - HTTP mode - Configure server to run in HTTP mode   [Default]
[X]  2 - HTTPS mode - Configure server to run in HTTPS mode


Do you want to continue Yes/No?
```

ACP over TLS

OCSDM primarily communicates with SBC using ACP (Acme Control Protocol). OCSDM supports ACP over TLS which adds a layer of security to the communications link between the SBC and OCSDM. Trusted and/or Entity Certificates must be configured during the installation/upgrade process with the Setup tool. To establish the TLS community for ACP, you must:

1) Import the valid Trusted CA Certificate to Session Delivery Manager for device authentication during the handshake.

2) If mutual authentication is enabled on your device, you must create a valid Entity Certificate for Session Delivery Manager to send the device during the handshake. To sign an Entity Certificate by the CA, you must perform the following steps, in order.

    a. Generate a Certificate Signing Request (CSR) and send the request to CA.

    b. Store the signed certificate reply from the CA on a local directory accessible to Session Delivery Manager.

    c. Import the CA (signer) certificate as a Trusted Certificate.

Import the signed certificate reply.

Please refer to Oracle Communications Session Delivery Manager Installation Guide 7.4 for the details of ACP over TLS.

Passwords

Default passwords are avoided in the OCSDM system. All passwords are obtained during system run-time, either during installation or during the application run-time. All the passwords obtained, generated, stored, or transmitted are encrypted using Password Based Encryption.

Chapter 3: Security Features

The OCSDM Security Management

The Security Manager slider in Session Delivery Manager manages the OCSDM user accounts and maintains the authentication and authorization policies for each user. Those users who have administration privileges are considered security administrators. They can access the different functions to manage users and audit logs.

User Management

User management lets you create new users and new user groups, and set group-based authorization where users are assigned to groups with different levels of authorization.

Setting authorization means you assign privileges to the group to which a user belongs. The privileges for that group are also assigned to all users who are members of the group. When a user logs into Session Delivery Manager, they can access functionality based on the privileges assigned to them.

The administrator is responsible for creating new user groups and users, and for controlling the different security levels of Session Delivery Manager by assigning privileges. Administrators can:

- Create user groups and users
- Assign users to groups that provide specific authorization policies to for all members of that group
- Provide fine-grained access control for specific groups, views, operations
- Limit the access for some users to specific features and functionality

Groups

A group is a logical collection of users grouped together to access common information or perform similar tasks. You assign specific permissions to a group and then assign users to it. Those users in turn, inherit the group-based permissions.

The following groups are created by default when Session Delivery Manager is installed:

- administrators: Super user group privileged to perform all operations
- LIAdministrators: Privileged to perform most operations including Lawful Intercept (LI) configuration changes. Privileges do not include changing the default

administrator user credentials. For example, users assigned to the default LI administration group cannot enable/disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups.

- provisioners: Privileged to configure SBCs and save and apply the configuration with the exception of a LI configuration.
- monitors: Privileged to only view data, both configuration and other kinds of data. They cannot configure SBCs. This group has the fewest privileges.

Users

A user is an individual who logs into Session Delivery Manager and performs a set of Session Delivery Manager- or application-related operations for which they have permission. Before a user can access Session Delivery Manager operations, they must be added as a user to the Session Delivery Manager server database. When you create users, you add them to user groups and the user privileges for that group will apply to them.

After logging into Session Delivery Manager, the operations available to a user are based on the group to which the specific user belongs.

Operations

Operations are all the tasks you can perform using Session Delivery Manager, such as configuring SBCs and performing administrative functions. They are logically arranged in a tree structure with parent and child operations (the Operations Tree) you access when creating group and user accounts. You provide or deny access to these operations by assigning a privilege to them.

Privileges

Privileges include allowing or disallowing a user from performing operations. Privileges are assigned on the group level and are propagated to all users who belong to the group. Please refer to Oracle® Communications Session Delivery Manager Administration Guide Release 7.4

Setting Inactivity timer to prevent unauthorized access

OCSDM offers and recommends setting inactivity timer to prevent unauthorized access to the system. The inactivity timer logs off the user from the OCSDM session when its value is exceeded. The user must re-enter their password to continue. You can set different values

for a user with administrative permissions and users who do not have administrative permissions.

The default value for an administrator account's inactivity timer is set to 0 (never expire). User must set a different value in order to terminate the user's session after a specified period of time. Please refer to Oracle® Communications Session Delivery Manager Administration Guide Release 7.4 for the details.

Audit logs

OCSDM's audit logs provides information about the changes made using Session Delivery Manager. The audit log contains audit trails. Audit trails enable you to view all operations that have been performed, the time they were performed, whether they were successful, and who performed them.

Thus audit logs help secure the system by constantly monitoring the access to the system. Users can view, search or save the audit logs on OCSDM user management menu. Please refer to Oracle® Communications Session Delivery Manager Administration Guide Release 7.4 for greater details on Audit logs for OCSDM.

Synchronizing System User passwords

As a security measure, users should periodically change the passwords. You can synchronize the OCSDM with changed passwords of system users using the Tools > Passwords dialog. Please refer to Oracle® Communications Session Delivery Manager Session Element Manager User Guide Release 7.4 for the greater details on this feature.

External AAA for RADIUS and Active Directory Configuration

External Authentication, Authorization, and Auditing/Accounting (AAA) enable users of OCSDM to utilize existing RADIUS or Active Directory servers for OCSDM user authentication. User groups that are created and managed externally must be mapped to internal OCSDM user groups. OCSDM local and external users are supported simultaneously, although external users do not have corresponding user records or username/password information stored in Session Delivery Manager.

The authentication, authorization and auditing mechanism allows administrators and LI administrators to edit external authentication settings.

For External AAA for RADIUS Configuration

- RADIUS server must be configured to use the same shared secret string for all SDM cluster nodes.
- RADIUS server must be configured to return one or more attribute values in the authentication response message to represent the groups a user belongs to.

For External AAA for Active Directory Configuration:

- Active Directory must be configured for LDAP over SSL if enabled in Session Delivery Manager.
- Active Directory must support version 5, if using the Kerbeos protocol.
- Each user object in your Active Directory must store the groups of each member using the "memberOf" attribute.

Please refer to Oracle® Communications Session Delivery Manager Admin Guide 7.4 for the greater details on External AAA, RADIUS and Active Directory configuration.

Chapter 4: Security Considerations for Developers

OCSDM offers Web Service which is a SOAP/XML Provisioning Application Programming Interface (API) enabling users to write applications that automate the provisioning of Session Border Controllers (SBCs). OCSDM Web Service consists of operations that can be performed against SBCs managed by an OCSDM server, and data structures used as input and output parameters to those operations. The operations are invoked by a client application to provision SBCs.

Please refer to Oracle® Communications Session Element Manager Web Services SOAP/XML Provisioning API Guide 7.4 for further details of secured web services programming on OCSDM. This document also provides a full description of the individual interface definitions that make up the API.

It is highly recommended that user fully secures the link between his Web services application (Web service client). It is also recommended that the application developers follow secured coding standards.

Appendix A: Secure Deployment Checklist

The following security checklist includes guidelines that help secure your system:

1. Do NOT connect your system to any untrusted networks, especially the Internet, until all protections have been configured. Customers have reported systems under configuration compromised in minutes due to incomplete configurations.
2. Harden the management environment.
    a. Make sure all equipment is in locked cabinets or at least in a secure room.
    b. Configure OCSDM's inactivity timer.
    c. Set strong passwords for all default accounts and OS system users (nncentral user, sudo, e-mail user, OCSDM's admin user, etc.) prior to configuration during product installation.
    d. Configure OCSDM's user management to limit access only to users that require access.
    e. Change the default SNMP community string and follow the SNMP configuration recommendations.
    f. Choose HTTPS as opposed to HTTP during product installation.
3. Practice the principle of least privilege.
    a. Carefully consider who has access to the admin password.
    b. Use mechanisms provided by the OCSDM to authenticate users or services accessing the system:
        i. Local authentication and authorization
        ii. RADIUS and active directory authentication.
    c. OCSDM comes with a few default user groups: monitor, provisioner, administrators and LIadministrators. Administrators are the only ones who have full set of permissions. The system provides role-based access control with dedicated user accounts that have pre-assigned privilege levels. These are discussed further in the section on management interfaces. The system provides local and remote authentication mechanisms and role-based security policies.
4. Monitor the system for unusual events.
    a. Configure the SNMP trap receiver.

b. Monitor system activity to detect problems with performance or availability as well as to determine when someone is attempting to abuse system services. Useful monitoring information can be acquired through audit logs, system logs, SNMP and RADIUS accounting.

5. Always deploy the product with the high availability and redundancy offered by OCSDM. High availability and resilience, key components of a secure deployment, help maintain service availability 24/7.

Appendix B: Encryptions and RNG used

Algorithm Name	Type (Symmetric or Asymmetric)	Bit Length	Purpose of the Algorithm. Describe what is encrypted (e.g. stored data, communications, management/ administration data , internal data, key transfer). Specify which encryption modes are supported (e.g., cipher feedback mode or cipher block chaining mode). If possible, provide example of usage of the encryption key.
MD5, SHA-1	Asymmetric	128	Provide HTTPS support via following offerings 1. Weak cipher SSL 2.0 2. Strong cipher SSL 3.0 3. Strong TLS1.0
OpenBSD-style Blowfish password hashing, described in "A Future-Adaptable Password Scheme" by Niels Provos and David Mazieres.	Symmetric	64	Used to encrypt stored passwords.
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,3des-ctr,arcfour,arcfour128,arcfour256	Asymmetric	128	SSH2 protocol support and SFTP support for file transfer between SDM servers and between servers to devices.