Brochure

Experience first-class protection

HP-UX Comprehensive Security

Hewlett Packard Enterprise

Experience first-class protection

In today's business environment you cannot afford to compromise security. Whether your business needs to run without interruptions or you handle data that needs to stay uncompromised, protecting your operating environment is vital. In the not too distant past, server security was a priority only for a small number of data centers, typically identified by highly sensitive data being processed, either financial or military in nature. More recently, IT managers across industries are being asked to take a closer look at their platform security because security breaches can cost time, money, and your businesses reputation and credibility, along with this there has been a rapid increase in regulatory mandates created to protect both your businesses and your customers.

Internal and external security threats leave your business vulnerable. In addition to your own desire to stay protected, many mandates have been put in place to ensure industry wide security levels are reached. Mandates affect you in almost all businesses and take many forms; from government imposed legislation such as Sarbanes Oxley (SOX) and Health Insurance Portability and Accountability Act (HIPAA), to industry-driven practices such as Payment Card Industry (PCI), to those requirements that are increasingly identified by in-house security or audit teams. In virtually all of these cases technology elements are necessary for your compliance with these mandates.

HP-UX 11i provides layered security with in-depth protection. It reduces risk from threats, simplifies identity management, and forms part of the compliance solution. In addition, the following benefits come with HP-UX security:

- **No extra cost:** HP-UX 11i security solutions are included in the cost of the OE and are offered to customers at no extra charge. We help reduce your risk without increasing your cost.
- **Improved performance:** Hewlett Packard Enterprise designs and delivers security solutions through targeted development, open-source, and third-party integration to provide excellent customer experience. Hewlett Packard Enterprise architects and tests HP-UX 11i security solutions for optimum performance.
- **Automated, integrated, and manageable:** Hewlett Packard Enterprise integrates HP-UX 11i security solutions into the OEs. Security is automated for ease of use and manageability, thus reducing the total cost of ownership (TCO).
- **Trustworthy:** HP-UX 11i including key partitioning technologies have been certified against the requirements for EAL4 Common Criteria.

Experience a comprehensive and well-integrated set of security features designed for greater protection against both internal and external threats aimed at proactively mitigating risk and reducing compliance cost. For the past three decades, Hewlett Packard Enterprise has been building one of the most trustworthy and secure UNIX® operating systems in the market.

To best protect your business and ensure you meet regulatory standards HP-UX has comprehensive security split into the following categories:

- **Protecting data:** Ensuring the integrity and confidentiality of data in transit, in use, and at rest.
- **Protecting systems:** From tools that protect a system against an attack, to those that detect and react to threats.
- **Protecting identity:** Securing the entire infrastructure by simplifying user authentication and access management, while auditing all privileged actions that take place.
- **Security Certifications:** Get the assurance offered by a neutral third party as to the diligence and quality with which we design and implement our HP-UX offerings.

This brochure is intended to provide an easily referenced overview of these categories and their features, along with the Software Depot download links and the necessary pointers to more in-depth information on the Hewlett Packard Enterprise Support Center.

Protecting data

Ensuring the integrity and confidentiality of data in transit, in use, and at rest

FEATURE	KEY BENEFITS
HP-UX Encrypted Volume and File Systems (EVFS) Address your data protection and compliance needs with HP-UX 11i Encrypted Volume and FileSystem (EVFS), by storing files in a way where they cannot be read by unauthorized parties who obtain physical access to your storage. It supports both volume-level encryption and file-level encryption; you choose whichever best fits your needs. Files and databases can be encrypted without the need to modify the applications accessing them. The storage media including tape and disk can be used without modification to store the encrypted files and databases. Additionally, you get highly efficient crypto processing by coupling the server multiprocessing and pipelining features of HPE Integrity Servers with HP-UX 11i. Even your sensitive business transactions can be stored in an encrypted format using the Advanced Encryption Standard (AES); AES is a block cipher adopted as an encryption standard by the U.S. government.	**Protect archived data** with strong AES encryption preventing the unauthorized use of data in storage obtained through theft, fraud, or unauthorized access. **Ensure compliance** with regulations on data retention and data protection by archiving and encrypting data with HPE Reference Information Manager (RIM). **Experience transparent encryption with easy management** of encryption keys through simple end user implementation, no application changes required and compatibility with most storage techniques: direct attach, network attached, storage area network. **Reduce cost** since you don't have to spend time and money erasing data. **Fully integrated** with HP-UX Serviceguard, HPE RIM, HPE Data Protector, HP-UX Trusted Computing Services (TCS), and most HP-UX supported storage devices.

To download HP-UX Encrypted Volume and File Systems and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Encrypted Volume and File Systems visit the **HPE Support Center**.

HP-UX Trusted Computing Services (TCS) Experience strong protection of your sensitive information as HP-UX Trusted Computing Services (TCS) provide software support for hardware-enforced key management on supported HPE Integrity servers. By providing a low-cost embedded security chip option, known as a trusted platform module (TPM), in its select Integrity servers, Hewlett Packard Enterprise has established a foundation for strong protection of sensitive information—including cryptographic keys. Built around industry standards, the TPM provides a basis for key storage by securely generating and storing cryptographic keys. HP-UX TCS takes this a step further by providing the necessary infrastructure for managing the TPM, as well as integrating it into select features such as HP-UX EVFS and HP-UX Secure Shell.	**Maintain security** in transparent encryption services while enabling High Availability features such as "auto-boot." **Builds the foundation for advanced security services** such as remote verification of hardware and software, for example, security policy auditing and reporting. **Increased protection of cryptographic keys** through strong, "machine-bound" protection to help eliminate vulnerabilities in software-only solutions. **Fully integrated** with HP-UX EVFS keys through a plug-in component, HPE Serviceguard for transparent migration into a cluster, a TPM OpenSSL engine that enables OpenSSL applications to use TCS RSA key pairs for hardware based security identification of servers; and sshd daemon using TPM protected private RSA key for server authentication. The embedded security hardware conforms with the Trusted Computing Group's TPM specifications v-1.1b, and the application APIs delivered as part of TCS conform to Trusted Computer Group (TCG) Software Stack specification version 1.21.

To download HP-UX Trusted Computing Services and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Trusted Computing Services visit the **HPE Support Center**.

Availability HP-UX 11i v3;
HP-UX TCS software requires an Integrity server with the TPM installed, this is currently supported on select Integrity servers, including (but not limited to): rx2800 i2, rx2800 i4, BL860c i2, BL870c i2, BL890c i2, BL860c i4, BL870c i4, and BL890c i4.

FEATURE	KEY BENEFITS
HP-UX Whitelisting Protect your system from unexpected downtime and denial of service by preventing inadvertent or illegitimate changes to the critical system files with HP-UX Whitelisting (WLI). It protects your files from unauthorized access by granting permissions only to the authorized applications, irrespective of the user (UID) executing the application. WLI is complementary to the traditional UNIX discretionary access controls (DAC) based on user, group, and file permissions. It is a cryptographic key-based product and its features are based on RSA key ownership and encryption technology. WLI security features are imposed through RSA signatures and enforced through signature verification. Therefore, regular files and directories may be protected from access by any user including the super user.	**Protect data integrity** by preventing the modification, deletion, and renaming of read-only critical files with File Lock Access Control (FLAC) policy, and restricting only trusted applications to access critical files to a specified set of applications with Identity Based Access Control (IBAC) policy for files residing on VxFS (also known as JFS), HFS, and NFS file systems. **Reduce security** threats by restricting access to critical system resources such as accessing kernel memory images (/dev/kmem and /dev/mem), dlkm, WLI metadata (WMD), and WLI APIs which manipulates the policies. **Simplify certification efforts** such as PCI-Data Application Data Security Standard (PCI-DSS) by preventing unauthorized access to critical data files. **Compatible with** Serviceguard clusters for high availability as well as HPE Data Protector and the Symantec NetBackup which means that WLI configuration and WLI meta-data can be backed up safely for future user reference.
HP-UX Security Containment Dramatically reduce the likelihood of system compromise with a suite of security technologies—HPE Security Containment for HP-UX 11i. These enhanced security features are incorporated into the mainstream HP-UX 11i operating environment to help your business combat increasingly complex threats. Without requiring modification to applications, HPE Security Containment isolates compromised applications, this also denied unauthorized access to other applications or files on the system. Security Containment comprises two core technologies that together provide a highly secure operating environment: compartments and fine-grained privileges. Compartments provide isolation and restrict access to application and system resources outside of the compartment to prevent catastrophic damage should a compartment be penetrated. Fine-Grained Privileges grant only the privileges needed for a task and, optionally, only for the time needed to perform the task.	**Stay protected even after an attack** with isolation of system resources and applications, even if the security of one application in compromised other system resources and applications remain secure. **Reduce total cost of ownership (TCO)** with the ability to partition for server reduction and consolidation and the confidence that unplanned downtime due to server compromise is practically eliminated. **No need to modify existing applications** as HP-UX 11i Security Containment is transparent at the application layer. **Integrated Security** when Containment is used with other applications to enhance the security of your HP-UX system.

To download HP-UX Whitelisting and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Whitelisting visit the **HPE Support Center**.

To download HP-UX Security Containment and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Security Containment visit the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX Containers (formerly SRP) Obtain isolated execution environments for consolidating multiple workloads within a single image of the HP-UX 11i operating system with HP-UX Containers (formerly HP-UX Secure Resource Partitions, SRP). Workloads within a container have user-defined entitlements to system resources such as CPU, memory, networking, storage, and file system. HP-UX Containers support multiple container types: A workload container provides a lightweight workload hosting environment. A system container provides many of the user-space capabilities of a virtual-machine guest without the associated management and performance overhead of managing an OS. And, an HPE 9000 container provides a binary emulation environment to run your HP-UX PA-RISC workloads on HPE Integrity hardware without recompilation.	**Increase Security** between workloads with isolated execution environments. **Reduce costs** by consolidating workloads running on separate servers onto a shared OS environment, reducing software license requirements, and having fewer OS instances to manage. **Improve system resource utilization** (such as CPU, memory, networking) and better utilize data center resources (power, cooling, footprint) by hosting multiple workloads on fewer servers. **Protect investments in legacy applications** with HPE 9000 containers by re-hosting PA-RISC applications on latest Integrity hardware.

To download HP-UX Containers and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Containers visit the **HPE Support Center**.

HP-UX OpenSSL Experience secure transfer of sensitive information over the Internet with the open standard security protocol Secure Socket Layer (SSL). SSL provides three things: privacy through encryption, server authentication, and message integrity. Client authentication is available as an optional function. HP-UX 11i operating systems implement the Secure Sockets Layer (SSL) v2/v3 and Transport Layer Security (TLS) v1 protocols using the OpenSSL Toolkit developed by the OpenSSL Project **openssl.org**.	**Enhance encryption capabilities** with various ciphers which can be used to encrypt or decrypt a message. HP-UX OpenSSL support the following ciphers: Blowfish, Carlisle Adams and Stafford Tavares (CAST), Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Data Encryption Standard Extension (DESX), Rivest Cipher 2 (RC2), and Rivest Cipher 4 (RC4). **Ensure content of your messages has not been altered** with the following message digest algorithms: Hashed Message Authentication Code (HMAC), Message Digest 2, 4, and 5 (MD2, MD4, and MD5) algorithm, RACE Integrity Primitives Evaluation Message Digest (RIPEMD) algorithm, Secure Hash Algorithm (SHA), SHA1, and SHA2. **Increase message security** with the following public key encryption methods: Rivest, Shamir, and Adleman (RSA) algorithm, Digital Signature Algorithm (DSA), and Diffie-Hellman (DH) algorithm. **Affirm that receivers can understand your messages** with support of the following file formats for encoding keys, certificated and digitally signed files: Abstract Syntax Notation One (ASN.1), Distinguished Encoding Rules (DER)—stores ASN.1 structures containing keys and certificates, Privacy Enhanced Mail (PEM)—stores keys, certificates, and encrypted files, Public-Key Cryptography Standard 7 (PKCS#7)—stores digitally signed files, PKCS#8—stores private keys, and PKCS#12—stores keys and certificates in browsers. **Support the following digital certificates:** X.509, X.509 version 3, and Certificate Revocation List (CRL). **Fully integrated** with the following HP-UX features: LDAP-UX Client, Apache-based Web Server, IPSec, AAA Server, TCS, Whitelisting, Secure Shell, Workload Manager, Strong Random Number Generator, and HPE WBEM Services for HP-UX.

To download HP-UX OpenSSL and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX OpenSSL visit the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX Secure Shell Log in more securely to another system over a network to execute commands on a remote system, and to move files from one system to another system using HP-UX Secure Shell. HP-UX Secure Shell is based on the open source Secure Shell (OpenSSH) product. OpenSSH is available in two versions: SSH Protocol Version 1 (SSH-1) and SSH Protocol Version 2 (SSH-2). HP-UX Secure Shell supports both versions of OpenSSH. SSH-2 is recommended because it is more secure than SSH-1. Key attributes of this secure connection are strong authentication, strong encryption, and public-key cryptography for communication between a client and the remote system, as well as a secure channel that the client uses to execute commands on the remote system. This secure access to a remote host enables you to execute commands safely on a remote system, move files from one system to another with increased security, and copy remote files more securely. With HP-UX Secure Shell you will be protected from the following potential threats to your business: IP spoofing, eavesdropping, and hijacking.	**Strengthen authentication** with support of two-way authentication: the server authenticates the client and the client authenticates the server. **Gain strong encryption** as communication between the client and the server is encrypted using intelligent, patent-free encryption algorithms such as Blowfish, DES, 3DES, and AES. **Avoid potential threats** with port forwarding allowing you to redirect the traffic through SSH secure channel between the client and server. **Protect vital data** with chroot directory jail which prevents users from changing application directories above that specified directory. **Simplify management** with agent forwarding facilitating secure key-based authentication using an authentication agent, this agent typically runs in the client environment and holds all key information, the only place in the network where the key information is stored is the local system, keys are never disclosed to any other component of the network. **Fully integrated** with PAM modules, Shadow passwords, Kerberos 5 and GSS-API, OpenSSL, audit logging, audit extensions, Strong Random Number Generator, TCP wrappers, RBAC keystroke logging, and LDAP-UX integration for host key management on 11i v2 and 11i v3, TPM hardware can be used to secure the host key on 11i v3, the /etc/utmp, /var/adm/wtmp, and /var/adm/btmp files, the /etc/default/security file and the /var/ adm/syslog/syslog.log file.
HP-UX IPSec Experience an infrastructure that allows secure communication—authentication, integrity, and confidentiality—over IP-based networks between systems and devices that implement the IPSec protocol suite. The IP security (IPSec) protocol suite was defined by the Internet Engineering Task Force (IETF) to provide security for IP networks. HP-UX IPSec is the HPE implementation of IPSec for the HP-UX operating system.	**Increase security** with host-based authentication which identifies the remote system through pre-shared keys or digital certificates. **Simplify management** as HP-UX IPSec is transparent to existing applications and there is no need to rewrite or reconfigure them. **Facilitate policy configuration** with a command-line interface that provides default parameter values that can be modified, flexible rule-based security attributes and access control policy configurations and batch mode for bulk configuration. **Compliant** with IPSec standards, including Internet Key Exchange (IKE) for automated key management. **Compatible** with most IPSec implementations, including those of Microsoft®, Cisco, and Linux®.

To download HP-UX Secure Shell and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Secure Shell visit the **HPE Support Center**.

To download HP-UX IPSec and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX IPSec visit the **HPE Support Center**.

Protecting systems

Arming you with a variety of tools ranging from ones that protect a system against an attack, to those that detect and react to threats.

FEATURE	KEY BENEFITS
HP-UX Software Assistant	
Consolidate and simplify patch management and security bulletin management on your HP-UX systems with HP-UX Software Assistant (SWA). This will help you answer compliance related questions such as "How do I evaluate, report on, and maintain the security bulletin compliance of my systems?" SWA is supported on HP-UX 11i systems and on Windows within HPE Systems Insight Manager (SIM). SWA can perform a number of checks including published security issues, installed patches with warnings, and missing patches with critical fixes. Once an analysis has been performed, you can use SWA to download any recommended patches or patch bundles, and create a depot ready for installation.	**Simplify and enhance security** with patch and security system analysis, suggested actions, and automatic patch selection. **Increase protection** by verifying patch integrity before unpacking downloaded patches. **Analyze your system and generate reports** with an HPE supplied catalog file or catalog downloads from non-HP-UX systems. **Speed-up analysis** by analyzing multiple systems at a time with HPE SIM 6.0.
HP-UX Bastille	
Ease your organizations' system-hardening security and/or regulatory-compliance activities, with protection against both known and unknown vulnerabilities using HP-UX Bastille. It guides customized lock downs via its wizard interface, addressing most of recommendations from a number of popular security scanning tools and checklists. Bastille can report the state of system configuration and detect a system-configuration "drift" from a saved "security-configuration baseline." With Bastille you also gain the ability to lock down a system interactively by answering a set of questions that each explains a security issue and describes the resulting action needed to lock down your system. Each question describes the cost and benefit of each decision and lets you decide how the tool should handle the issues. After you answer all of the questions, Bastille performs the requested lock-down steps that are automatable. Both reporting and system lockdown can be performed non-interactively and help you with security auditing.	**Increase security** against both known and unknown vulnerabilities by reducing the attack surface for defense against unknown vulnerabilities and configuring and enabling Software Assistant for defense against known vulnerabilities. **Prevent intrusion** by locking down system easily and repeatedly by securing daemons and system, reducing unneeded services such as pwgrd, educating users through the user interface, configuring Security Patch Check or Software Assistant to run automatically and configures an IPFilter-based firewall, etc. **Identify new threats** by using drift feature to identify the change in the configuration. **Restore to good state** using the baseline and drift features. **Fully integrated** with System Insight Manager, HP-UX Install-Time Security, Software Assistant/ Security Patch Check, HP-UX IPFilter, and HP-UX Standard-Mode Security Extensions. **Dependency:** HP-UX Perl D.5.8.0.A or higher—Use Perl D.5.8.8.8 for better performance.

To download HP-UX Software Assistant and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Software Assistant visit the **HPE Support Center**.

To download HP-UX Bastille and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Bastille visit the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX Install-Time Security Ensure your system is secure from the first installation. HP-UX Install-Time Security is an "out-of-the-box" security-lockdown choice from four security levels during the installation process. This is done by integrating HP-UX Bastille with Ignite-UX and Software Distributor (SD). It allows you to choose between one of four levels depending on your needs: "Network DMZ"—appropriate for deployments in that part of your network, or any other higher risk environments, including large intranet environments, "Managed DMZ"—applies the Network DMZ lockdown, but enables common system management protocols, "Host"—a functional lockdown that disables many services and protocols not in common use or "Tools-Only"—pre-enables the system for later lockdown, but applies no configuration change.	**Speed-up and secure deployment** with "secure-by-default" installation even into high threat environments. **Customize your security and compatibility decisions** to suit your needs, with one of four levels. **Integrated** with Ignite/UX, HPE Software Distributor, Update/UX, HP-UX Bastille, Software Assistant, HP-UX IPFilter, and HP-UX Secure Shell.
Boot Authentication Make it possible to configure a system so that only authorized users are allowed to boot your machine into a single-user mode. A site's security policies may require you to authenticate before you can boot a system into single-user mode. This product now provides secure single-user mode with root password protection, but without the overhead of converting the system to trusted mode. For this feature to work, the boot authentication feature must be enabled before you reboot the system.	
HP-UX Auditing System The HP-UX Auditing System is a part of the operating system intended to record instances of privilege operations requested by the user on the system, in the form of system calls. It provides the audit logs in real time or offline mode on a disk. The HP-UX Auditing System helps in addressing common security requirements of most compliance regulations such as SOX, PCI, SB1386, and HIPAA. The HP-UX Auditing System and its extensions act as a deterrent against system abuses and expose potential security weaknesses by enabling the administrator to record events selectively for analysis and detection of security breaches providing you with auditing generated records that are the best source of system and user activities on the host. Take advantage of filtering and reporting functionality for optimal resource utilization and better management of your logs with HP-UX Auditing System Extensions.	**Increase boot security** with the ability to safely boot your system into single use mode. **Protect the host from physical abuse** where hackers can take over by booting the machine into single user mode. **Facilitate regulatory compliance and detection of malicious activities** that help in forensic analysis and in compliance with SOX, PCI, SB1386, and HIPAA. **Reduce cost while managing audit data** using built-in reporting and web-based reporting. **Optimizes resource utilization with audit filtering** which reduces the audit I/O activities using filtering feature to increase performance, and by selectively recording events for lower disk usage. **Ease log management integration** with APIs to convert raw-audit data into desired format. **Enhance filtering and reporting** with the HP-US Audit System Extensions for HP-UX 11i v3.

To download the HP-UX Install-Time Security functionality of HP-UX Bastille and learn more visit the **Software Depot**.

For documentation and manuals on the HP-UX Install-Time Security functionality of HP-UX Bastille please visit the **HPE Support Center**.

To download Boot Authentication and learn more visit the **Software Depot**.

For documentation and manuals on Boot Authentication visit the **HPE Support Center**.

To download HP-UX Auditing System Extensions and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Auditing System Extensions visit the **HPE Support Center**.

HP-UX System Administrator's Guide: Security Management in the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX IPFilter	
Control packet flow in or out of a machine with a stateful system firewall that filters IP packets, HP-UX IPFilter. It works as a security defense by cutting down on the number of exposure points on a machine.	**Protect your system** on an intranet against internal attacks as well as external attacks that have breached perimeter defenses. **Increase flexibility** with an alternative to the restricted configuration of Internet Services. **Protection from Distributed Denial of Service DDOS attacks** using Dynamic Connection Allocation (DCA) functionality. **Gain NAT support** for address translations.
HP-UX Host IDS	
Proactively monitor, detect, and respond in near real-time, to both known and unknown attacks that originate from the network or on the host with HP-UX Host Intrusion Detection System (HIDS). It protects the host from a hacker attempting to break into or disrupt the system, subversive "insider" activities, or someone trying to spread a virus. This product relies on the audit records generated by the HP-UX audit sub-system which is the best source of system and application activities. It provides a simplified usage and management interface with a predefined surveillance schedules (configuration) to facilitate quick and easy deployment, a command-line and GUI administrator tools for managing and monitoring multiple HIDS agents, and a command-line tool for facilitating the fine-tuning of schedules/configuration.	**Stay continuously protected** with surveillance against system misuse or intrusion. **Complement your network-based security solutions** by detecting intrusions that network-based security products cannot identify due to encrypted payloads or that originate from the host, "insider" attacks. **Help meet regulatory standards** such as PCI Data Security Standard and Sarbanes-Oxley (SOX) by having HIDS monitor critical resources and system activity. **Customizable**, intrusion response with tailored alert in different formats (HTML, text, so on) and surveillance schedules to implement server-specific security policy. **Integrated** with the HP-UX audit system to provide near real-time detection based on high-quality audit records and HPE OpenView Operations (OVO) to manage and monitor multiple HIDS sensors centrally from the OpenView Console.
HP-UX Standard Mode Security Extensions (SMSE) (Password policies)	
Extend the security capabilities of "trusted mode" into the new HP-UX Base Operating Environment with Standard Mode Security Extensions (SMSE). It provides many new security features in standard mode HP-UX, including most of the security features that were previously available only on systems that were converted to trusted mode.	**Ensure protection** with the userstat (1m) command which checks the status of local accounts and reports abnormal status, such as account locks. **Increase security flexibility** as security features can be individually configured to apply system wide or to specific users. **Help address compliance regulation** that impose strict security policies for password, user logins, etc. **Integrated** with HP-UX Security Containment, HP-UX RBAC, and HP-UX Shadow Passwords.

To download HP-UX IPFilter and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX IPFilter visit the **HPE Support Center**.

To download HP-UX Host IDS and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Host IDS visit the **HPE Support Center**.

To download HP-UX Standard Mode Security Extensions (SMSE) and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Standard Mode Security Extensions (SMSE) visit the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX Shadow Password	
An increase in the computational power available to hackers has made the non-hidden passwords in the UNIX /etc/passwd file vulnerable to decryption. Shadow Passwords enhances your system security by hiding user encrypted passwords in a shadow password file. Encrypted passwords previously stored in the publicly readable /etc/passwd file can be optionally moved to the /etc/shadow file, which is accessible only to privileged users.	**Increase security** with shadow passwords hidden from non-privileged users leaving them less vulnerable to decryption. **Simplify configuration** once Shadow Password is installed the pwconv(1m) and pwunconv(1m) command can be run to enable shadow passwords, and the pwunconv(1m) command can be run to disable shadow passwords. **Supported with the following:** HP-UX Security Containment, HP-UX RBAC, HP-UX Standard Mode Security Extensions, LDAP-UX, and NIS (HP-UX 11i v3 only).
HP-UX Strong Random Number Generator	
Remove the potential security threat of generating encryption keys from non-random sources. HP-UX Strong Random Number Generator (SRNG) provides a secure, non-reproducible source of true random numbers for applications with strong security requirements, such as for generating encryption keys. The /dev/random and /dev/urandom files created by this product allow the read(2) system call to retrieve strong random binary sequences of up to 256 bytes. When configured to use these special files, applications such as SSH and OpenSSL will have a more secure environment for performing cryptographic computations.	**Stay continuously protected** with surveillance against system misuse or intrusion. **Complement your network-based security solutions** by detecting intrusions that network-based security products cannot identify due to encrypted payloads or that originate from the host, "insider" attacks. **Help meet regulatory standards** such as PCI Data Security Standard and Sarbanes-Oxley (SOX) by having HIDS monitor critical resources and system activity. **Customizable**, intrusion response with tailored alert in different formats (HTML, text, so on) and surveillance schedules to implement server-specific security policy. **Integrated** with the HP-UX audit system to provide near real-time detection based on high-quality audit records and HPE OVO to manage and monitor multiple HIDS sensors centrally from the OpenView Console.
HPE Secure Development Lifecycle Code Signing	
Ensure all your software is authentic with an HPE signature on all new HP-UX software. Software delivered through an Operating Environment (OE) or the AR media is now digitally signed using HPE's private key. You can verify the authenticity of the software before or during installation of an OE or products delivered through the OE or AR media. For more information, see Ignite-UX and SD administration guides. Starting April 2013, all the software and patches that shall be shipped by Hewlett Packard Enterprise will be digitally signed and can be verified for authenticity before, or during installation.	**Increase security** by identifying unwarranted software before or during installation. **Guaranteed authentic HPE software** as administrator can restrict HP-UX host to have only "authenticated software."

To download HP-UX Shadow Password and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Shadow Password visit the **HPE Support Center**.

To download HP-UX Strong Random Number Generator and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Strong Random Number Generator visit the **HPE Support Center**.

For documentation and manuals on HPE Secure Development Lifecycle Code Signing visit the **HPE Support Center**.

Availability: HP-UX 11i v3 (update release 12 or later)

Protecting identity

Securing the entire infrastructure by simplifying user authentication and access management, while auditing all privileged actions that take place.

FEATURE	KEY BENEFITS
HP-UX Role-Based Access Control (RBAC) How do you allow multiple administrators without compromising on security? Multiple administrators often lead to problems such as shared root passwords, lack of accountability, and the increased potential for system compromise, as all the administrators have access to everything. This issue is often raised in compliance-related audits and is an important issue to address. A main function of RBAC is the ability to distribute select administrative responsibilities while maintaining security and accountability. It provides an alternative to the traditional "all-or-nothing" root user model, while allowing creation of roles with just the appropriate authorizations.	**Simplify usage and management** with predefined configuration files to facilitate quick and easy deployment, privileged shells make privilege elevation transparent and command-line and Web-based management with System Management Homepage. **Customizable** through pluggable architecture for customizing access control decisions and integrating existing access control policy information and flexible re-authentication ability through PAM allowing restrictions on a per-command basis. **Fully integrated** with HP-UX 11i Security Containment (Fine-Grained Privileges and Compartments), select HP-UX commands and HP-UX audit system for a single, unified audit trail.
PAM Kerberos Allow multiple authentication technologies to coexist with Pluggable Authentication Module (PAM) Kerberos providing Kerberos authentication as per the PAM architecture that is specified in Open Group RFC 86.0. PAM. A /etc/pam.conf configuration file determines the authentication module to use that is transparent to the applications that use the PAM library.	**Seamless integration** with Kerberos domain for authentication using PAM-Kerberos without any changes, using this module, HP-UX users can be integrated with Windows ADS domain for authentication.
Kerberos Client Implementing secured client/server applications in either 32-bit or 64-bit development environment with the Kerberos Client (KRB5CLIENT) software, including libraries, header files, and utilities.	**Gain thread safety** for Kerberos libraries. **Simplify management** of service tickets in the credential cache. **Support powerful cryptographic algorithms** such as 3DES, RC4, and AES. **Compatible** with IPv6 and TCP.

To download HP-UX RBAC and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX RBAC visit the **HPE Support Center**.

To download PAM Kerberos and learn more visit the **Software Depot**.

For documentation and manuals on PAM Kerberos visit the **HPE Support Center**.

To download Kerberos Client and learn more visit the **Software Depot**.

For documentation and manuals on Kerberos Client visit the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX LDAP-UX Client Integrate HP-UX into existing identity management infrastructures with LDAP-UX Client Services. LDAP-UX addresses key compliance requirements through a shared identity infrastructure that includes unified passwords and universally enforced password policies, integrated provisioning and de-provisioning of users and rights, and versatile access rights management. Integration with existing infrastructures includes support for off-the-shelf directory server products, including Windows Active Directory, as well as support for customer-defined data models.	**Easy to use and manage** with setup wizard for quick installation and options for detailed data model description and security configuration, in addition, a configuration profile allows a single configuration to be shared across multiple HP-UX hosts for rapid deployment. **Customizable** as you can define a configuration profile that describes the deployed LDAP data model, allowing HP-UX to share OS information with other directory-enabled applications, define descriptive access policy to determine user access and authentication rights on the HP-UX OS and its services, use dynamic groups to define access rights to files or applications, enable encrypted SSL/TLS access to directory server data to protect authentication and OS information and lastly benefit from flexible re-authentication ability through the Pluggable Authentication Module (PAM) that allows restrictions on a per command basis.
HP-UX AAA Server Experience enhanced security for wired and wireless LAN access, authentication and accounting for virtual private network (VPN) gateways, firewalls, and other network devices with the Remote Authentication Dial-In User Service (RADIUS)-enabled middleware and applications of HP-UX AAA Server. HP-UX AAA Server is a powerful, full-featured RADIUS server solution for enterprise, telecommunications, and other environments requiring centralized authentication, authorization, and accounting of user access to services.	**Increase security and flexibility** by choosing the right authentication methods based on your security policies: password, digital certificates, or token cards as well as through support of a varied number of authentication mechanisms using Network Access Servers or Switches of Wireless Access Points, wireless LAN EAP authentication including PEAP, TLS, TTLS, GTC/OTP, MSCHAP, MD5. **Comply with regulations** by enabling OATH standards-based two-factor authentication and IPv6, DHCP, and SNMP support. **Better performance** with multi-server management using Web-based console, shared multi-sever session state and accounting, failover while preserving existing sessions as well as scalability and high availability using multiple servers. **Enable integration into your existing databases** with supports of LDAPv3, ODBC-compliant databases (including Oracle and MySQL), and flat file user data stores. **Customizable** with finite state machine architecture, software Development Kit (SDK) for developing your own RADIUS server features, highly configurable Advanced Policy Engine and Livingston, Merit, and custom accounting formats.

To download HP-UX LDAP-UX Client and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX LDAP-UX Client visit the **HPE Support Center**.

To download HP-UX AAA Server and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX AAA Server visit the **HPE Support Center**.

FEATURE	KEY BENEFITS
HP-UX Directory Server Simplify security by centralizing user profiles, application settings, and group data into a network-based registry using the Lightweight Directory Access Protocol (LDAP) compliant server software for HP-UX Directory Server (HPDS). It improves security by enabling administrators to store policies and access control information in the directory for a single authentication source across enterprise intranet or extranet applications.	**Simplify use and management** with a graphical console to manage server and directory as well as a command-line tool with scripting for updates and other modifications to enterprise directory server and its content. **Increase availability** with a multi-master replications for both read and write operations. **Benefit from features** such as chaining and referrals to increase the power of the directory by storing a complete logical view of the directory on a single server while maintaining data on a large number of directory servers, transparently to clients as well as multiple authentication methods, password policy and account lockout and database encryption supports encryption of selected attributes within a database. **Fully Integrated** with the advanced identity integration capabilities of the HP-UX 11i OE, HPDS makes the perfect repository to manage networked OEs, also integrated with the Windows® User Sync feature, which synchronizes changes in groups, users' entries, attributes, and passwords between the HPDS and Microsoft Active Directory Server.
HP-UX Kerberos Server Designed to provide you with a strong authentication for client or server applications using the shared secret key cryptography, HP-UX Kerberos Server is available as part of the Kerberos security product family. Kerberos is a mature network authentication protocol based on the RFC 1510 (The Kerberos Network Authentication Service (V5)) specification of the Internet Engineering Task Force (IETF).	**Strengthen authentication** where you can be assured that users, who log in to your network are who they claim to be, to access the services, databases, and applications on your client-server network. **Ensures high availability** of mission critical applications, in the event of the primary server crashing or going down, the secondary server (backup) can immediately be made the primary server. **Increase scalability** as multiple secondary security servers can be configured to enable load balancing with automatic incremental propagation, without any performance degradation. Realms can be organized according to types of users or services. **Enhance system performance** with pre-threaded concurrent server which includes a pool of threads to simultaneously service multiple client requests in the key distribution center. **Increase security** with 3DES encryption, a much stronger encryption than the 56-bit DES. **Automatically update** incremental changes from your primary server to the associated secondary servers, synchronizing both the servers. **Integrated** with IPv6 address support, Windows 2000 interoperability, LDAP database, and C-Tree database.

To download HP-UX Directory Server and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Directory Server visit the **HPE Support Center**.

To download HP-UX Kerberos Server and learn more visit the **Software Depot**.

For documentation and manuals on HP-UX Kerberos Server visit the **HPE Support Center**.

Security Certifications

Get the assurance offered by a neutral third party as to the diligence and quality with which we design and implement our HP-UX offerings.

FEATURE	KEY BENEFITS
Common Criteria Certifications	
Security certifications provide an independent validation of the HP-UX security model. HP-UX 11i has a long history of achieving security certification including a recent EAL4+ Common Criteria certification with commercial off the shelf (COTS) Compartmentalized Operations Protection Profile-Operating Systems (CCOPP-OS). This certification specifies an extensive range of security requirements with a much broader scope than previous certifications, including twice the number of functional requirements. HP-UX 11i v3 is Common Criteria certified against CCOPP-OS. This profile specifies an extended range of protection requirements for vital partitioning functions, namely compartments with mandatory access controls (MAC), vPars, and nPars. It also extends the list of successful HP-UX certifications that already include CAPP/RBAC protection profiles.	**Validate our claims** with external security certifications. Ensure the following key technologies are certified through HP-UX Common Criteria CCOPP-OS certification: • Compartments provide isolation of process, memory, and files within a single instance of HP-UX 11i should an attack compromise a portion of the OS, MAC is included. • Virtual partitions (vPars) are soft partitioning solutions that provide granularity and flexibility to cell-based servers, it allows multiple instances of HP-UX 11i to run independently within an nPartition. • Hard partitions (nPartitions or nPars) are previously included in HP-UX 11i v3 certified configuration for CAPP/RBAC and are also included in CCOPP-OS, each nPartition provides both hardware and software isolation, so that hardware or software faults in one nPartition do not affect other nPartitions within the same server complex.

Developing solutions for major social and environmental challenges
hp.com/hpinfo/globalcitizenship

Technology Services Support for HP-UX

HPE Technology Services helps build an infrastructure that is reliable, highly available, and rooted in proven best practices, and offers a support experience that:

- Proactively avoids problems by leveraging automation and online tools
- Provide faster problem resolution with integrated HW and SW support and dedicated team of experts
- Optimize performance and enhance efficiency with a range of per event services
- Keep your systems up-to- date with delivery of new updates

HPE Technology Services Portfolio:
HPE Technology Services support portfolio offer three levels of on-going customer support services and a comprehensive family of added value service offerings that customers can deploy as needed.

Foundation Care: Reactive hardware and software support services provides integrated hardware and software support, and choice of response times, coverage windows, and length of term options.

Proactive and Mission Critical Services: Innovative, higher value support services that offer high performance reactive support, proactive support, remote and onsite support and consultations with HPE technology experts for 24x7 availability.

Datacenter Care: For environmental level support customized for customers' unique business needs. This service offers flexible support service designed to help customers consistently meet service-level targets and other business objectives.

Lifecycle Event Services: Per-event services that reduce customer's time to value with deployment services, and help optimize the performance of IT infrastructure.

For more information, go to:

- **HPE Technology Services**
- **HPE Datacenter Care Services**

Learn more at
hp.com/go/hpuxsecurity

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA4-5937ENW, April 2016, Rev. 1