Hitachi Content Platform Anywhere Security
Whitepaper

By Hitachi Data Systems

August 2014
Contents

Executive Summary ................................................................. 4
Overview ..................................................................................... 5
User Access and Security ......................................................... 6
  End User and Administrative Authentication .................................... 6
  End User Access via Desktop ....................................................... 6
  End User Access via Mobile Clients ............................................ 6
Admin Controls ........................................................................... 6
  Clear Credentials ........................................................................ 6
  AD Status Change ...................................................................... 6
  Disable User ............................................................................. 7
  Delete User ............................................................................. 7
End User Controls ....................................................................... 7
  Client and Device Controls ....................................................... 7
  Device Access ......................................................................... 7
  Deregister Device ..................................................................... 7
  Data Wipe ............................................................................. 7
  Browser Access Timeouts .......................................................... 7
  Maintenance Access ................................................................. 8
Data Security Controls ............................................................... 8
  Data In Flight Encryption .......................................................... 8
  Certificate Management ............................................................ 8
  Data at Rest Encryption ............................................................. 8
  Versioning/User Self-Service Restore .......................................... 9
  Audit Logging ........................................................................ 9
Data Sharing .............................................................................. 9
  Folder Sharing ....................................................................... 9
Executive Summary

In the world of cloud and data mobility, there is an expectation that information can be accessed anytime, anywhere, and from any device. While this was originally driven in the form of public cloud services, enterprise users quickly took advantage of these services as corporate IT struggled to keep up.

This user driven move to store corporate assets in the public cloud was not without risk. Corporate information began to leak into public clouds outside of the traditional enterprise security perimeter and stored in places that lacked an appropriate level of enforceable security and compliance.

Since no one doubts the advantages of mobile data access for business advantage and agility, Hitachi Data Systems offers the ability for enterprises to allow their users to securely access anytime, anyplace, and from any device through HCP Anywhere.
Overview

HCP Anywhere is a file sync and share (FSS) application. The primary purpose is to provide the ease of use of a consumer-class FSS product such as Dropbox, with enterprise class functionality that organizations can host securely on-premises. At the core of HCP Anywhere is the Hitachi Content Platform (HCP) object store that provides the security foundation of this offering.

A fundamental design goal for HCP Anywhere is to be “simply secure”. This means that HCP Anywhere is designed with security as core tenet of its development. HCP Anywhere allows ease of user experience and the enforcement of organizational security policies simultaneously.

This document will describe the security aspects of the HCP Anywhere product related to secure access to the system, secure access to data, and protection from threats as well as data corruption.

Figure 1: HCP Anywhere Architecture
User Access and Security

HCP Anywhere controls user access by leveraging existing authentication and authorization infrastructure in the customer environment.

End User and Administrative Authentication

With HCP Anywhere, administrators and end users are authenticated against Active Directory (AD) via the Kerberos protocol. HCP Anywhere maintains lists of authorized AD Groups that are permitted to access the system. Each user that requires access must be a member of at least one authorized AD Group. When logging into the User Portal or Management Console, the user’s credentials are authenticated against AD. If single sign-on is properly configured on the user’s browser, and the user is located in a network that is able to access the AD domain server, the user’s current Kerberos ticket is used for authentication allowing the user to bypass the logon screen.

End User Access via Desktop

On Windows and Mac clients, the user must provide login credentials when initially registering. The credentials are authenticated and from this a Kerberos ticket is created. The ticket is used with AD to permit the HCP Anywhere client application on these clients to connect to the HCP Anywhere server without prompting the user for login information. By default, the ticket is valid for a specific period, after which the user is prompted to re-enter their login information and a new ticket is created. The clients do not store the user credentials once authentication is done.

End User Access via Mobile Clients

On mobile clients, Android, iOS and Windows Phone, when registering the device with the HCP Anywhere server the user is required to provide their AD login information which is validated by the HCP Anywhere server. The mobile device then receives the same type of security ticket as is used on the desktop clients. This permits the HCP Anywhere app on the mobile to connect without needing to prompt the user for login credentials. Again, this ticket is valid for a specific period after which the user is prompted to re-enter their login information. In addition, an HCP Anywhere profile is deposited on the mobile device that enforces lock code usage on the device. System administrators control the policy for whether a lock code is required on Android and iOS devices, as well as the lock code length and type (alphanumeric or just numeric).

Admin Controls

Clear Credentials

At any time an administrator from the Management Console can issue the clear credentials command against any and all devices for a particular user. Once issued, regardless of single sign-on configuration or security token validity, the user will be prompted for login credentials the next time that the HCP Anywhere client attempts any communication with the HCP Anywhere server.

AD Status Change

The user’s status must remain intact within AD in order to be authenticated. A user will lose the ability to authenticate and then access HCP Anywhere if:

1. Their valid user account is removed from all AD groups that are registered with HCP Anywhere
2. Their user account is expired in AD
3. Their user account is deleted from AD
In all of these cases, the user will lose access to HCP Anywhere from mobile clients and browsers. Their desktop clients will still permit access to their data, but will no longer synchronize with the HCP Anywhere server. Administrators can take additional action to wipe the HCP Anywhere data from any and all user devices.

**Disable User**

At any time, an administrator from the Management Console can choose to disable a particular user in HCP Anywhere. At that point, all user clients will no longer be able to synchronize with the HCP Anywhere server. They will still be able to access the data on their desktop clients, and cached data on their mobile clients, but any changes made will not be sent to the HCP Anywhere server for synchronization. Once a user is re-enabled, all normal operations resume and any changes made while the user was disabled will now synchronize.

**Delete User**

At any time an administrator can issue a choose to delete a particular user in HCP Anywhere. Once this happens, the user will no longer be able to authenticate and access the HCP Anywhere server. All the user’s devices will lose access and no longer be able to synchronize with the HCP Anywhere system. Optionally if chosen, the user’s data will be deleted from the HCP Anywhere system. The data will remain accessible on the user’s desktop. The data will be inaccessible from mobile clients. Deregister Device commands can be issued by an administrator prior to the Delete User command in order to wipe the data from any and all devices. Additionally, deleted users can be re-enabled on the system if needed.

**End User Controls**

**Client and Device Controls**

HCP Anywhere provides a variety of client and device controls to enforce security no matter how end users want to access their data.

**Device Access**

Each user is permitted to register up to a specified number of devices (desktop and mobile) with the HCP Anywhere server.

**Deregister Device**

At any time the user or an administrator may deregister any registered device. On the next network communication with the HCP Anywhere server, the deregistered device will note its state change and no longer synchronize with the HCP Anywhere server. There are also configurable system settings which will allow deregistration of inactive devices after certain days with options to delete data from user’s desktop clients.

**Data Wipe**

If the user issued the deregistration, the data on the device will be wiped when it receives the deregistration command. If an administrator issued the wipe, the administrator can decide if a data wipe should be performed. By default, the wipe occurs.

**Browser Access Timeouts**

Administrators can set a configurable inactivity timeout period for user and management console browser access. After timeout, the user is auto-logged out of their browser session.
Maintenance Access

Should a circumstance arise such that HDS support personnel need to access the HCP Anywhere server, measures are in place to ensure that access is secure. Support can only access the system via SSH. The HCP Anywhere administrator must first enable the port from the HCP Anywhere Management Console for that access to occur. On connecting to SSH, Public Key authentication logon is required. The support person will use the private key and password known only to HDS support. New key pairs are generated with each release of HCP Anywhere.

Data Security Controls

Data In Flight Encryption

Data flows from the HCP Anywhere clients to the HCP Anywhere server until it can be moved to a Hitachi Content Platform (HCP) object Store for storage. No copies of the data remain on the HCP Anywhere server.

As data moves between the client and the HCP Anywhere server, all network communication occurs over TLS sessions (for desktop clients) or HTTPS with TLS (for browser access) to prevent eavesdropping or tampering. To protect data in transit, HCP Anywhere server uses a secure tunnel protected by 128-bit or higher strong symmetric encryption ciphers. Data in transit between a client and the server is always encrypted. The customer can determine how this encrypted network traffic is terminated.

There are three options for implementing data-in-flight encryption on HCP Anywhere as follows:

1. The TLS protocol session can take place from the client all the way to the HCP Anywhere server.
2. The TLS protocol session can take place from the client to the customer’s load balancer/firewall, terminate there, then transition to an unencrypted socket connection to the HCP Anywhere server.
3. The TLS protocol session can take place from the client to the customer’s load balancer/firewall, terminate there, then transition to a new TLS session (with a new key) from the load balancer to the HCP Anywhere pod.

It should also be noted that the communication from the HCP Anywhere server to the HCP object store can optionally be configured to communicate via HTTPS using TLS.

Certificate Management

The HCP Anywhere server allows customers the choice of using self-signed or trusted 3rd party certificates. HCP Anywhere can generate a Certificate Signing Request if required or certificates can be uploaded in PKCS12 format. Optionally self-signed certificates can also be generated. The mobile and desktop connections will leverage these certificates for secure transmission of data to and from HCP Anywhere.

Data at Rest Encryption

1. HCP Anywhere’s storage device, the HCP system, can be configured to encrypt all data at rest within it. Data at Rest is encrypted using 256-bit AES.
2. All HCP Anywhere data on iOS clients is natively encrypted on disk without option by iOS itself. Please refer to “iOS Security 2012” published by Apple Inc.
3. HCP Anywhere itself currently does not perform data at rest encryption on the other client devices. HCP Anywhere clients are compatible to operate with corporate deployed disk encryption software technologies.
Versioning/User Self-Service Restore

To protect users from accidental file/folder deletion or unwanted file content changes, HCP Anywhere has a versioning and user self-service restore capability. For any folder, a user can view a list of deleted items and choose to restore any of them. For any file, a user can view a history of changes to the file including the ability to open and view the historical file’s contents. The user can select any prior version of a file and restore it to become the current version.

Administrators can set limits on the versioning policy. The administrator can set both the length of time that any particular historical version remains accessible in the system, and the number of historical versions that remain accessible in the system. These parameters operate independently. That is, if a prior version is only allowed to remain for 3 months, then after 3 months it will be removed from the system even if there are fewer prior versions of the file than the maximum allowed in the system.

Audit Logging

HCP Anywhere provides detail auditing of the data and actions for each user in the HCP Anywhere system. An administrator who has been assigned the role of “Auditor” can do an Audit against any user. The auditor can review:

1. All of the users files and folders, including the files contents
2. All of the user authentication attempts
3. When/which files have been shared by a link and whether shared privately or publically
4. Any shared link access attempts. For private links, the user attempting access is captured in the log.
5. All file and folder activity, create, update, delete, rename, etc. This information is available for all the data in a user’s private HCP Anywhere folder, folders that the HCP Anywhere user has shared with others, and shared folders owned by others to which the HCP Anywhere user is a member.

Data Sharing

Folder Sharing

An HCP Anywhere user can share their HCP Anywhere folders with other registered HCP Anywhere users in the system. The HCP Anywhere users can be a member of up to 100 folders that are owned by other HCP Anywhere users. A single shared folder also includes all files and sub-folders of that shared folder, currently, with no exclusions of files for sub-folders.

1. All HCP Anywhere users participating in the shared folder have full CRUD (create, read, update and delete) access to the folder contents.
2. All HCP Anywhere users participating in the shared folder can view a list of other participants including the folder owner.
3. All HCP Anywhere users participating in the shared folder can view a detailed activity log for themselves and other users of the shared folder.
4. At any time a participant of a shared folder may choose to leave the shared folder. When the leave folder operation is executed, the contents of the folder will be wiped from all of the user’s devices on next communication with the HCP Anywhere server.
5. At any time the Owner of a shared folder may remove a user from the shared folder. Again, this action will automatically wipe the folder data from all of the user’s devices on next communication with the HCP Anywhere server.

6. At any time the Owner of a shared folder can unshared the folder. On this action, all other users of the shared folder will lose access and have the folder contents removed from their devices. The folder and its data remain available to the folder Owner.

Link Sharing

A second sharing capability for HCP Anywhere users is “link sharing”. An HCP Anywhere user can request HCP Anywhere to create a link to any of the user’s files within their HCP Anywhere folder. Shared links have the following properties:

1. **Internal Link**: The receiver of an Internal link has to be a registered HCP Anywhere user and is prompted to provide valid AD credentials that are validated before the link will be resolved. This is the default behavior.

2. **Public Link**: If the HCP Anywhere user chooses the “Public” link option, then any receiver of the link will be able to download a copy of the file. Note, HCP Anywhere administrators can choose by policy to disallow public link sharing.

3. **Expiration Date**: The HCP Anywhere user must specify a number of days that the link will be active. After the specified number of days, the link will no longer be valid.

4. **Manage Link**: The HCP Anywhere user can view their existing active links and choose whether to expire or extend a particular link.

5. HCP Anywhere administrators can define the policy for Link Sharing usage. The policy enforces:
   a. Allow link sharing of any type (Internal or Public)
   b. Allow Internal link sharing only and disallow Public link sharing
   c. Maximum period that any link can be active for in HCP Anywhere
   d. Default period that a link is active for in HCP Anywhere

HCP Object Store Security

The HCP Anywhere stores its data onto the HCP object store and takes advantage of its legacy of offering enterprise class security. Anywhere leverages the multi-tenancy capabilities of HCP such that all of the Anywhere data is isolated to its own private tenant. Within the Anywhere tenant inside HCP, Anywhere creates additional private namespaces to securely store the user files and backup copies of the HCP Anywhere database. These namespaces can only be accessed by the HCP Anywhere system.

A properly configured HCP has many additional features to safeguard that integrity of the data. These features, taken in aggregate, ensure that the system does not require backup

Availability

HCP tracks each object in a database distributed across all HCP nodes (minimum of 4) with each node containing a shard of the database and a different shard owned by another node. The shards and shard copies are stored on separate groups of disks to ensure that failure of a whole disk group will not cause the loss of both the primary and copy of any
particular shard. If a single shard is lost, it can quickly be regenerated from its copy. With this design, HCP is protected from losing its ability to find objects on the system. This design is referred to as Metadata Protection Level 2 (MDPL2).

Local Replication

HCP can be configured to keep 1, 2, or 3 additional copies of each object. This selection can be made on a per-namespace basis. This is referred to as Data Protection Level (DPL). Similar to MDPL, each copy of any particular object is placed on different sets of disk to protect from object loss in the case of group disk loss. Should an object become lost or damaged, HCP automatically repairs the object from a local replica (or a remote replica).

Remote Replication

HCP supports asynchronous remote replication. Separate and different DPL policies can be defined on the primary HCP and remote replica HCP systems. As mentioned above, any lost or damaged object is automatically repaired from a replica object.

Data Integrity

HCP scans all objects on a regular basis for integrity. It captures and stores separate hashes for the file and custom metadata that make up the object. If during a scan, an object is found to no longer match its hash, it is automatically repaired from either local or remote object replicas.

Versioning

HCP namespaces can be configured to keep prior versions of a named objects. Should an accidental object deletion occur, the object can be restored from a prior version.

HCP Anywhere Deployment

Here we describe elements of the HCP Anywhere to enable secure deployment within a company’s IT environment.

Separated Front End/Back End Networks

The HCP Anywhere servers have physically separate network interfaces/ports:

1. **Front End Network**: Used for communicating with HCP Anywhere clients. This traffic may be coming in over the Internet and/or routed over internal networks. As described earlier, this traffic should be configured through the company load balancer/firewall infrastructure and the HCP Anywhere server supports multiple options for SSL termination.

2. **Back End Network**: Used for communicating on company’s private internal network. It provide connection to the HCP storage system, DNS, AD, NTP server, and Virus Scanning Engine.

HCP Anywhere Node Hardening

1. HCP Anywhere software makes no direct SQL calls. All database functionality is passed through stored procedures to prevent SQL injection attacks

2. HCP Anywhere is validated against an industry standard vulnerability scanner to identify and resolve common security issues such as:
   - Weak SSL ciphers
   - Form injection attacks
   - XSS attacks

Hitachi Data Systems
3. Product code upgrades are online, fast, and customer executable. This enables rapid reaction to any newly discovered security threat.

4. Monitoring of system access attempts via both the User Portal and Management Console so that a user or administrator can spot suspicious activity.

**Virus Scanning**

The HCP Anywhere server can be configured to communicate to a corporate virus scanning engine (Symantec, McAfee, and Trend Micro). When an HCP Anywhere user adds/changes a file on their client, the file is sent to the HCP Anywhere server. BEFORE storing that file and making it available to all the other devices for that user, the HCP Anywhere server forwards the file to the virus scanner using the ICAP (IETF.ORG RFC 3507) protocol. If the virus scanner deems that the file is infected and requires to be quarantined, then the file will not be synchronized by the HCP Anywhere server. On the user client where the file was added, an HCP Anywhere synchronization error status will be raised identifying the file as containing a virus.

**Port Documentation**

The customer is provided with complete documentation of all required and optional network accesses to/from HCP Anywhere server so that the network admins can perform port lock down in accordance with company policy.

**Conclusion**

Security is a core tenant of HCP and the Anywhere system. HDS is committed to continue expanding the security capabilities of HCP Anywhere in future versions of the product while maintaining a positive user experience for end users and administrators alike.