ASUS CLOUD CORPORATION

ServiceGateway

Version 09.06

Austin Chen

2009

Rm. 817, 8F, No. 53, Minquan Rd., Yonghe Dist., New Taipei City, Taiwan

Content

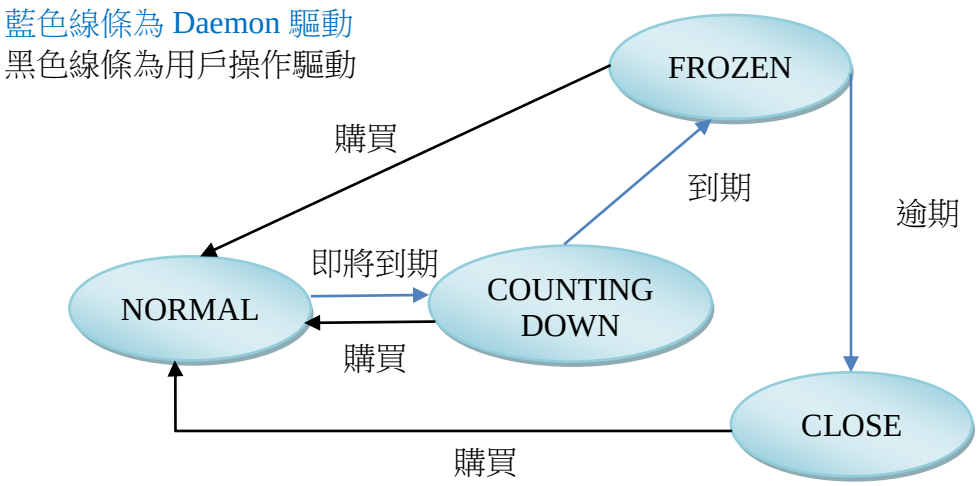
ServiceGateway 功能簡介

ServiceGateway 主要功能在於調度一個 Service Area 內實際提供服務的主機，針對該 Service Area 內的使用者，ServiceGateway 會分配一組適合的相關伺服器位址。

ServiceGateway 中用來授權驗證 (Acquire Token) 使用者的 API 是「/member/acquiretoken/」，該 API 會回傳 Token、InfoRelay 以及 WebRelay 的位址給客戶端。接著，客戶端便可以帶著 ServiceGateway 所核發的 Token 自由使用 InfoRelay 和 WebRelay 提供的 API 開發 ASUS WebStorge 的相關服務。

ASUS WebStorge 用戶遍佈全球，著眼於各 Service Area 內某特定之服務的使用期限，帳號可以分為數種狀態：NORMAL State、COUNTING DOWN State、FROZEN State 及 CLOSE State。

帳戶使用期限狀態圖



帳戶使用期限狀態的定義

- **NORMAL State**：

  為 ASUS WebStorage 的正常狀態，檔案上傳下載及系統相關功能皆可正常使用。用戶可按照購買系統使用權時之契約執行所有功能。

- **COUNTING DOWN State**：

  距離使用期限少於指定的時間長度(目前訂為 15 天)之即將到期狀態。

- **FROZEN State**：

  該狀態是指用戶已屆使用期限，未再購買使用時數。FROZEN 狀態最長維持 1 個月，此段期間內用戶的資料仍被保存於系統內。在此狀態中，用戶無法上傳檔案。

- **CLOSE State**：

  用戶在 FROZEN 狀態超過 1 個月仍未購買使用時數，則該用戶之帳號將被關閉。於此狀態下，Acquire Token 雖可取得有效的 Token，但用戶檔案及其目錄將被清除，亦無建立目錄或上傳檔案的功能，讓用戶可接受系統的提示購買訊息。此時，可透過購買使用時數回到 NORMAL 狀態。

Auxiliary Password(CAPTCHA、OTP)機制

CAPTCHA

用戶登入 ASUS WebStorge 系統輸入之帳號(User ID)或密碼(Passowrd)組合若不相符且超過系統設定的容許錯誤次數，則系統會自動增加另一個圖型驗證碼傳送給客戶端，用戶必須輸入正確的 User ID / Password / CAPTCHA 字串才可以通過身份驗證，此機制可以預防存心不良的客戶端以 ROBOT 用各種帳號密碼組合不斷嘗試自動登入系統，藉此提高系統安全性。

OTP(One-Time Password)

為了提供用戶更高的資安服務水準，ASUS WebStorage 整合了 VIP (Verisign Identity Protection) WEB Services。對於要採用更嚴密資安防護的用戶，當其登入 ASUS WebStorge 系統時，除了必須填寫傳統的帳號(User ID)、密碼(Password)之外，還必須輸入一個限用一次的密碼，或稱為 OTP，三者皆合法時才可登入 ASUS WebStorge 系統。

1. 若用戶有購買 OTP 驗證服務，則將輸入資料的 OTP 及用戶的 Credential ID(請參閱下方註釋)，並將此 Credential ID 登錄於 VeriSign VIP Service 網站，使其成為一個有效的 Credential ID，並送往 VeriSign Web Service 進行 OTP 驗證。
2. 若用戶未購買 OTP 驗證服務，且輸入密碼錯誤累積超過次數，則進行身份認證時需要加入 CAPTCHA 圖型驗證碼以提高系統安全性。

※ Credential ID：經由安裝於用戶的手機、網頁瀏覽器等等的外掛程式，是根據機器硬體資訊產生的 ID。

ServiceGateway API 簡介

客戶端在使用 ASUS WebStorage 時須經過幾個步驟：

一、 首先，客戶端必須先向 ServicePortal 取得本身所屬之 Service Area 的 ServiceGateway 位址。

註:透過呼叫 ServicePortal 的/member/requestservicegateway/可以達成這個目的。

二、 接著，客戶端需要帶著使用者的帳號(User ID)和密碼(Password)，透過 ServicePortal 取得的 ServiceGateway 位址進行/member/acquiretoken/呼叫。

1. 將客戶端傳來的使用者帳號密碼進行認證。
2. 若帳號密碼無誤,則 ServiceGateway 核發的 Token 將伴隨著 InfoRelay、WebRelay 的位址回傳給客戶端。

為減少對 ServicePortal 的存取,客戶端可以在首度取得 ServiceGateway 位址後便儲存在本地電腦,直到發生客戶端無法連上先前儲存的 ServiceGateway 時再重新向 ServiceGateway 詢問所在地的 Service Area 內的 Service Gateway 位址。

本文件 API 閱讀須知

此段落將說明如何閱讀本文件的 XML Payload (即各個 API 的 Input、Output)。

- 以/member/requestservicegateway/為例：

<requestservicegateway>
<userid>{ User ID }</userid>
<password>{ 使用者密碼轉成小寫再做 MD5 編碼[註1]的結果 }</password>
<language>{ 使用者的語系，例如：*zh_TW* }</language>
<service>[*1*]</service>
</requestservicegateway>

閱讀說明：

標籤欄位	說明
<userid>{ User ID }</userid>	參數欄位可輸入的值以**{ }**做為表示。 如左例：若 User ID 為 test123@gmail.com，則 Payload 為 <userid>test123@gmail.com</userid>

- 以/fsentry/getentryinfo/為例：

<getentryinfo>
<token>{ token }</token>
<isfolder>[*0* | *1*]</isfolder><!-- 0：表示為 File ID | 1：表示為 Folder ID -->
<entryid>{ File ID | Folder ID }</entryid>
</getentryinfo>

閱讀說明：

標籤欄位	說明
<isfolder>[*0* | *1*]</isfolder> <!-- 0：表示為 File ID | 1：表示為 Folder ID -->	參數欄位**[ ](中括號)**的***斜體字***表示為實際上參數欄位可出現的值，並以**<!---->**補充說明文字。 如左例：[*0* | *1*]意指可輸入 0 或是 1。

API 說明(需 SSL 加密)

使用者帳號密碼身份認證

(/member/acquiretoken/)

目的：接受客戶端認證的要求，透過使用者帳號、密碼的驗證，以取得授權金鑰(Token)，並回傳此 Service Area 中各 Server 的位址，以進行其他 API 的操作。

/member/acquiretoken/這個 API 會給予客戶端一個在後續執行任何 API 時，用來驗證用戶身份所必須的 Token。除此之外，另一個重要的功能是提供所在之 Service Area 內各種伺服器的位置資訊給客戶端，目前計有下列數種伺服器的位置會透過這個 API 回傳給客戶端程式：

1. InfoRelay：在 Payload 中以<inforelay>表示，記錄 InfoRelay IP 位址與埠號。支援檔案、目錄的新增、刪除和修改名稱…等，處理無關檔案實體內容異動的作業。
2. WebRelay：在 Payload 中以<webrelay>表示，記錄 WebRelay IP 位址與埠號。提供了檔案上傳下載相關的服務。
3. Search Server：在 Payload 中以<searchserver>表示，記錄 Search Server IP 位址與埠號。支援檔案、目錄名稱的搜尋。

開發者授權傳送規格：

- 在 Cookie 中指定 sid 欄位，Cookie 中的「sid」必須為小寫英文字母。
- 在 Header 中必須帶入 Authorization Header，包含 signature_method、timestamp、nonce 以及 signature 四個參數。
  - **signature_method**：hash 的方式，目前提供以 HMAC-SHA1 演算法做 Hash。

- **timestamp**：從 1970/01/01 00:00:00 到現在為止的毫秒數。
- **nonce**：唯一且僅有的亂數，此值在 60 分鐘內不可重覆出現相同的值。
- **signature**：將上述三參數，依字母排列規格以 Query String 方式串接後做 URLEncode，再以 **ProgKey** 為 Key 值，進行指定 signature_method 的 **Hash** 演算，再將 Hash 過的字串加以 **Base64** 的轉換，最後再將 Base64 後的結果，再進行一次 **URLEncode** 的字串，即為 signature 字串。

※ 上述細節可參考 OAuth 實作規則中各參數內容的設定方式。

※ 若您使用的開發語言為 Ruby，請用 Base64.strict_encode64，避免 “\n” 在編碼之後出現。

系統會透過指定的 signature_method，將以上三參數串接並演算後與 signature 比對，若發現內容不相等，則會得到 Status = 5 的錯誤代碼。

※ URLEncode 後的結果字串中，所有 16 進位的英文字 (A~F) 都必須為大寫，否則進行 Hash 後的結果會有所不同。

Ex：

```
Authorization:    signature_method="HMAC-SHA1",
                  timestamp="1191242096",
                  nonce="kllo9940pd9333jh",
                  signature="%2FZtwu6IWV6jYtgPT9EjXJzwGV6Q%3D"
```

※ 在產品未取得本公司上市授權前，限定僅能存取指定的測試帳號內資料；而開發測試帳號請自行透過 ASUS WebStorage 產品註冊、啟用後，再申請 sid / ProgKey，並填寫申請單以進行開通 (至多五個測試帳號)；否則即使 sid、ProgKey 通過驗證，仍會因帳號不在清單中，而得到 Status = 5 的狀態碼。

回傳的狀態碼(Status Code)：

0 Success。

2 User Authentication Fail。

5 Developer Authentication Fail。(例如：sid 不存在或 ProgKey 驗證失敗。)

504 OTP 認證失敗。

也就是輸入的 User ID / password / OTP 不正確或須使用 OTP 認證卻未輸入 OTP。

505 OTP 服務的 Credential ID 處於 LOCKED 狀態。

508 CAPTCHA 認證失敗，或密碼輸入錯誤次數已超過系統設定值，使用者必須輸入 CAPTCHA，進行驗證。

999 General Error。

/member/acquiretoken/
Input
http header: Cookie:ONE_VER=1_0; sid=12345; path=/ **http body:** <?xml version="1.0" encoding="utf-8"?> <aaa> <userid>{ User ID }</userid> <password>{ 使用者密碼轉小寫經 MD5 編碼[註 1]後的字串 }</password> <time>{ time stamp, this is for scramble the payload }</time> <auxpassword>{ 僅在進行 Auxiliary Password 驗證流程中才須指定。若為 OTP 則此欄填 one time password；若為 CAPTCHA 則此欄填寫使用者輸入對應前次傳送給用戶的 CAPTCHA 的明文字串 }</auxpassword> <!-- auxpassword 只有在使用 OTP 或 CAPTCHA 驗證流程時才需要 --> </aaa>
Output
http header: Set-Cookie: OMNISTORE_VER=1_0; **http body:** <?xml version="1.0" encoding="utf-8"?> <aaa> <status>{ Status Code }</status>

```
    <token>{ token }</token>
    <!-- 以下 IP:PORT 資料，不填寫 PORT 時預設值為 80 -->
    <inforelay>{ InfoRelay 的 IP:PORT Ex: 192.168.1.201:8081 }</inforelay>
    <webrelay>{ WebRelay 的 IP:PORT }</webrelay>
    <searchserver>{ Search Server 的 IP:Port }</searchserver>
    <package>
        <id>{ Package ID }</id>
        <display>{ EeePC-20G }</display><!-- package name -->
        <capacity>{ 容量大小。Ex:2000 }</capacity><!-- 計量單位 MB -->
        <uploadbandwidth>{ 頻寬。Ex:128 }</uploadbandwidth><!-- 計量單位
        KB -->
        <downloadbandwidth>{ 頻寬。Ex:128 }</downloadbandwidth><!-- 計
        量單位 KB -->
        <upload>{ Ex:128 }</upload><!-- 計量單位 MB -->
        <download>{ Ex:128 }</download><!-- 計量單位 MB -->
        <concurrentsession>{ # 幾個 session(數值) }</concurrentsession>
        <maxfilesize>{ 數值 }</maxfilesize><!-- 單位為 MB -->
        <hasencryption>[ 0 | 1 ]</hasencryption >
        <expire>{ 到期日(格林威治時間)，yyyy-MM-dd HH:mm:ss }</expire>
        <maxbackuppc>{ 備份電腦數上限 }</maxbackuppc>
    </package>
    <!-- 當 Status Code 為 504、508 時表示必須使用 Auxiliary Password 驗證 -->
    <auxpasswordurl>{ 若為 OTP 則此欄為空字串 | 若為 CAPTCHA 則此欄為
    圖型驗證碼的 URL(網址經過 URL encoded) }</auxpasswordurl>
    <time>{ time stamp, this is for different the payload }</time>
</aaa>
```

使用者帳戶資訊(/member/getinfo/)

目的：查詢使用者基本資料及已使用狀況資訊；包括可用空間、已使用空間、可設定備份電腦數、已設定備份電腦數等資訊。

OTP Credential State 常數：

30 ENABLED ：被 Activate、Enable、Unlock 後，可正常使用的狀態。

20 DISABLED ：被 Disable，不可使用。

10 LOCKED ：輸入 OTP 錯誤過多次，被 VesiSign 鎖定，暫時不可用，直到以 Unlock API 解鎖定。

0 INACTIVE ：被 Deactivate，不可使用。

回傳的狀態碼(Status Code)：

0 Success。

2 Authentication Fail。

999 General Error。

/member/getinfo/
Input
http header: Cookie:OMNISTORE_VER=1_0; path=/ **http body:** <?xml version="1.0" encoding="utf-8"?> <getinfo> <userid>{ User ID }</userid> <token>{ token }</token> <time>{ time stamp, this is for scramble the payload }</time> </getinfo>
Output
http header: Set-Cookie: OMNISTORE_VER=1_0; **http body:** <?xml version="1.0" encoding="utf-8"?> <getinfo> <status>{ Status Code }</status> <account>{ Account ID }</account>

<email>{ Email Address }</email>
<regyear>{ regYear }</regyear><!-- 此值目前固定為 2008 -->
<language>{ *zh-tw* }</language>
<activateddate>{ 啟用時間，格式為 yyyy-MM-dd HH:mm:ss }
</activateddate>
<credential>{ 用戶的 OTP Credential ID }</credential><!-- 未使用 OTP 機制的用戶此欄為空字串 -->
<credentialstate>{ 用戶 OTP Credential ID 的現行狀態 }</credentialstate><!--未使用 OTP 機制的用戶此欄為空字串 -->
<usedbackuppc>{ 個數 }</usedbackuppc><!-- 此帳號已使用的備份電腦資料夾個數-->
<backuppc><!-- 此 Element 可重覆多次 -->
<name>{ 備份電腦的資料夾名稱的 Base64 編碼結果字串 }</name>
<!-- 若您使用的開發語言為 Ruby，請用 Base64.strict_encode64，避免“\n”在編碼之後出現。-->
<createdtime>{ 格式為 yyyy-MM-dd HH:mm:ss }</createdtime><!-- 備份電腦建立時間 -->
</backuppc>
<package>
<id>{ Package ID }</id>
<display>{ EeePC-20G }</display><!-- package name -->
<capacity>{ 容量大小。Ex:20000 }</capacity><!-- 計量單位 MB -->
<uploadbandwidth>{ 頻寬。Ex:128 }</uploadbandwidth><!-- 計量單位 KB -->
<downloadbandwidth>{ 頻寬。Ex:128 }</downloadbandwidth><!-- 計量單位 KB -->
<upload>{ Ex:128 }</upload><!-- 計量單位 MB -->
<download>{ Ex:128 }</download><!-- 計量單位 MB -->
<concurrentsession>{ # 幾個 session(數值) }</concurrentsession>
<maxfilesize>{ 檔案上傳容量上限 }</maxfilesize><!-- 單位為 MB -->
<hasencryption>[*0* | *1*]</hasencryption>
<expire>{ 到期日(格林威治時間)，yyyy-MM-dd HH:mm:ss }</expire>
<maxbackuppc>{ 備份電腦數上限 }</maxbackuppc>

```
        <featurelist>
          <feature name="{ 功能名稱，例如：MEar }" enable="[ 0 | 1 ]"><!--
          feature 可以重覆出現多次描述多個功能項目 -->
              <property name="{ 功能屬性名稱 }" value="{ 功能屬性
              值 }"/><!-- property 可以重覆出現，多次描述多個功能屬性 -->
          </feature>
        </featurelist>
    </package>
    <usedcapacity>{ 已使用空間 }</usedcapacity><!-- 單位為 MB -->
    <freecapacity>{ 剩餘可用空間 }</freecapacity><!-- 單位為 MB -->
</getinfo>
```

服務區域 ID 列表

服務區域 ID	服務區域
1	台灣
2	美國
3	大陸

回傳的狀態碼(Status Code)

Status Code	Description
0	Success
1	Version is not supported
2	Authentication Fail
3	Payload is not validate
5	Developer Authorization Fail
501	Illegal state
502	Unauthorized Remote IP
504	OTP 認證失敗。也就是輸入的 User ID/password/OTP 不正確或須使用 OTP 認證卻未輸入 OTP
505	OTP 服務的 Credential ID 處於 LOCKED 狀態
506	用戶啟用的 Credential ID 數量超過系統限制(一個帳戶只能有一個 Credential ID)
507	不合法的 Credential ID
508	CAPTCHA 認證失敗
999	General Error

註解

1. MD5 編碼注意事項

若您的 MD5 編碼未經過十六進制轉換，請務必在 MD5 編碼過後，再以十六進位轉換。十六進位所使用的「a,b,c,d,e,f」字母須為小寫。