

Comprehensive security shield

Mission Control Application Gateway, Mission Control Firewall, Mission Control Internet Proxy, Mission Control Security Gateway, **Mission Control Passport**, Mission Control Intrusion Detection, Mission Control Email Shield, Mission Control Virus Protection, Mission Control Client VPN, Mission Control Wireless Zone Protector



Mission Control Passport Datasheet Description

The Mission Control Passport answers **user and client authentication** requests. The authentication type is based on **username/password** and ideally extended with **one time token codes**. Users are administrated in the Mission Control Portal.

The **user and group management GUI** of the Mission Control Portal is shown in the following figure. It offers full user **administration and debugging** features to designated administrators. They can edit the user's credentials, define group permissions and set usernames and passwords. Lost and broken tokens can be **replaced** and new **token orders** are placed within the same application. The Passport fully integrates into the Active Directory environment by keeping the user in sync.

User List | Advanced User List

Show 20 Users

Login	Name	Email	Token Serial (Replacement)	Last Attempt
[redacted]	[redacted]	[redacted].com	7676247-5	29.07.2007 10:15
[redacted]	[redacted]	[redacted].com	6540362-4	07.09.2006 14:00
[redacted]	[redacted]	[redacted].om	12-0850618-9	
[redacted]	[redacted]	[redacted].om	12-0850619-6	
[redacted]	[redacted]	[redacted].n	6540365-5	01.08.2007 09:58
[redacted]	[redacted]	[redacted].com	6540361-7	08.07.2007 12:37!
[redacted]	[redacted]	[redacted].om	6540364-8	27.06.2007 14:20
[redacted]	[redacted]	[redacted].om	6540363-1	
[redacted]	[redacted]	[redacted].m	6540423-2	26.07.2007 23:03
[redacted]	[redacted]	[redacted].m	5035660-7	01.08.2007 03:51
[redacted]	[redacted]	[redacted].om	7676273-4	08.06.2007 19:53
[redacted]	[redacted]	[redacted].om	12-0836601-1	13.07.2007 18:34
[redacted]	[redacted]	[redacted].i	7672292-9	31.07.2007 01:47
[redacted]	[redacted]	[redacted].n	7672298-1	02.08.2007 14:12
[redacted]	[redacted]	[redacted].om	6540442-3	02.08.2007 14:28
[redacted]	[redacted]	[redacted].n	8372115-1	08.06.2007 21:14
[redacted]	[redacted]	[redacted].n	7672300-1	02.08.2007 14:45
[redacted]	[redacted]	[redacted].com	7672299-8	21.05.2007 19:17
[redacted]	[redacted]	[redacted].com	7672297-4	22.12.2006 15:07
[redacted]	[redacted]	[redacted].n	7676272-7	11.07.2007 13:36

Edit User

Personal and Contact Information

First name: Last name:
 Direct Phone: Mobile Phone:
 Home Phone: Fax:
 Email: Job Title:
Please enter telephone numbers in international format. e.g. + 41 1 1234 5678

Login Information

Login: Locked: yes no
 Password: Confirm (opt.):
Please choose a password of at least 6 characters in length and use a combination of characters, numbers and special characters.

Authentication

Type: Password-only Authentication Password and One Time Token temporarily allow password only
 Current Token: token lost or broken
 Replacement Token: ?

Group Memberships

[None] the user does not belong to any groups
 cvpn Client VPN
 cvs CVS Access
 mail Email Access
 mssadmin MSS Admin Access
 office Office Environment

Client VPN Group membership

(default) profile-defined default group
 -mobile Corporate Access for Mobile Users
 -corp Corporate VPN Client Access
 -dev-ext Web Development on gosting by external parties
 allow any group (help)

The **permissions** to administrate users can be **delegated** to designated user administrators which may be for example HR or the helpdesk. Every change to the user database is traceable in the audit trail log.

Each login attempt from every user is logged and available in the **real-time log viewer**. It explicitly shows accepted and rejected authentication attempts on a per user granularity. Thus, user administrators are quickly able to determine the exact cause of every failed authentication.

```

Users > Log
Authentication Log Client VPN Log IPass Log Audit Trail
Log for user: rz View log on host: tag (home)
Jun 19 07:51:08.706998: INFO: auth request (id=58): login='[redacted]', nas_id='[redacted]', nas_ip='[redacted]', client_ip='127.0.0.1', client_port='49222'
Jun 19 07:51:08.710841: INFO: login credentials (id=58): login='[redacted]', method='Password/Digipass', password='>.....', token_code='490714', service_groups='office,assadmin,cvpn,mail'
Jun 19 07:51:08.774701: INFO: auth accept (id=58): login='[redacted]', nas='[redacted]', nas_groups='*'
Jun 19 08:33:01.362450: INFO: auth request (id=247): login='[redacted]', nas_id='corp.[redacted]', nas_ip='[redacted]', client_ip='127.0.0.1', client_port='33575'
Jun 19 08:33:01.365676: INFO: login credentials (id=247): login='[redacted]', method='Password/Digipass', password='>.....', token_code='258194', service_groups='office,assadmin,cvpn,mail'
Jun 19 08:33:01.443023: INFO: auth accept (id=247): login='[redacted]', nas='corp.[redacted]', nas_groups='office'
Jun 19 09:02:49.23506: INFO: auth request (id=11): login='[redacted]', nas_id='fire.[redacted]', nas_ip='[redacted]', client_ip='127.0.0.1', client_port='60438'
Jun 19 09:02:49.29509: INFO: login credentials (id=11): login='[redacted]', method='Password/Digipass', password='>.....', token_code='706344', service_groups='office,assadmin,cvpn,mail'
Jun 19 09:02:49.105515: INFO: auth reject (id=11): login='[redacted]', nas='[redacted]', nas_groups='assadmin', reason='DPCHECK: Validation Failed (rc: 1)'
Jun 19 09:03:01.87001: INFO: auth request (id=11): login='[redacted]', nas_id='fire.[redacted]', nas_ip='[redacted]', client_ip='127.0.0.1', client_port='60438'
Jun 19 09:03:01.90963: INFO: login credentials (id=11): login='[redacted]', method='Password/Digipass', password='>.....', token_code='706343', service_groups='office,assadmin,cvpn,mail'
Jun 19 09:03:01.150969: INFO: auth reject (id=11): login='[redacted]', nas='[redacted]', nas_groups='assadmin', reason='password mismatch'

```

Specific applications communicate with Mission Control Passport via the **RADIUS** protocol.

The following two figures show the **graphical and statistical connection monitoring**. The graphical overview reports the availability per month, colored in uptime, ISP outage and connection down. Clicking on one pillar opens the details as shown in the second figure. It lists every outage and the corresponding ticket if the escalation threshold was reached and consequently **escalated to Mission Control**. All escalations can be configured to be notified per e-mail, text messages or fax.



The Mission Control Passport is running on dedicated **industrial strength hardware** for reliable 7x24h operation. The **hardened operating system** assures that only essential tools and utilities are activated and therefore cannot lead to unexpected instability and compromised systems. Mission Control further makes sure that all appropriate security related settings are up to date and configured correctly.

After extensive testing procedures, all required security updates and patches are installed, ensuring that the systems are always up-to-date. The device is capable of **booting multiple releases**, which provides an efficient fallback and recovery process if required. Furthermore, all device and environment specific configurations are **automatically generated**, based on the Mission Control operated **configuration database**. This is an essential part for an **efficient disaster recovery process** since it enables to generate and reinstall the identical configuration in a very short time.



High Availability

High Availability adds another instance of hardware that acts as an authentication server. Each additional server is updated and held in sync with the primary. They all have therefore exactly the same user database and are operated in two different ways:

- The main and the High Availability device share a virtual IP address. In the event of an incident with the primary device, the virtual IP address will **automatically switch over** to the other device and answer all authentication requests. This is the preferred option if geographic proximity allows a virtual IP address setup.
- The main and the High Availability device have different IP addresses. This scenario is used in geographic different locations within different networks. In this case, the clients send their request to the primary server and switch to the secondary if they do not get a response.

Passport Token

Passport tokens provide a constantly alternating 6-digit number that provides an additional authentication factor. It serves as a **one-time password** and therefore prevents various attacks on the user's credentials including keyboard logging at Internet Cafés or any eavesdropping and password thefts. Users are relieved from difficult password handling. Periodic password renewal enforcements can be simplified with even increased protection.




Active Directory Integration

This module integrates the Mission Control Passport into the existing Active Directory environment. It **synchronizes the users** including name, phone number, e-mail address, client VPN groups, authentication groups, job title, cost center and the password. Alternatively, the password can be excluded from synchronization and **polled** in real time on each request.

Token E-Shop

With the Token Shop, Passport tokens are **ordered online** within the Mission Control Portal. It allows defining the destination addresses of each token order and sending the tokens **directly to the users worldwide**. The following figure shows a snapshot of a token order.

Users > Token Shop

User List	Advanced User List	Token List	Token Shop	Synchronization	Audit Trail
Order > Review > Confirmation					
Token Information					Mission Control Tokens Please specify quantity, token type, and delivery options (shipping type and country) to receive total fees.
Quantity	<input type="text"/>				
Token Type	<input checked="" type="radio"/>  Digipass Quantity in stock: 97				
Billing and Delivery Information					
Billed Service ?	<input type="text" value="Passport (Level II, CHF) - Hosts: [redacted]-auth"/>				
Cost Center	<input type="text"/>				
Delivery Country	<input type="text"/>				
Delivery Address	<input type="text"/> or <input type="text"/>				
Delivery Option	<input checked="" type="radio"/> Standard Shipping <input type="radio"/> Priority Shipping				
Billing Address	<input checked="" type="checkbox"/> Same as above <input type="text"/> or <input type="text"/>				
Terms and Conditions	As on previously signed token shop annex.				
Additional Comments					
Order placed by	<input type="text"/>				
Comments	<input type="text"/>				
<input type="button" value="Review Order..."/>					<input type="button" value="Cancel"/>