**NEW JOINER DOCUMENT**

|  |  |
| --- | --- |
| Author: | **Manuel DYJA** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Version | **ID** | **Date** | **Description** |
| Creation | 0.9 | 11.02.2019 | Initial release |
| Modification | 0.91 | 29.08.2019 | Added NSO Keepass |
| Modification | 0.92 | 09.10.2019 | Added Skype GRANT and jumpserver |
| Modification | 0.93 | 20.10.2019 | Jump server, Safe list, LDN domain account groups, NSO wiki Link |
| Modification | 0.94 | 12.12.2019 | LPM GRANT |
| Modification | 0.95 | 23.07.2020 | New SNOW Queue/EMEA UT Code |
| Modification | 0.96 | 23/09/2020 | Added EMA/ASIA network & security devices access |
|  |  |  |  |

# Table of Content

[Table of Content 2](#_Toc101359991)

[**1.** **Administrative** 5](#_Toc101359992)

[**1.1.** Office access 5](#_Toc101359993)

[**1.2.** CA-CIB and WIPRO attendance 6](#_Toc101359994)

[**1.3.** eLearning 6](#_Toc101359995)

[**2.** **GRANT Habilitation** 7](#_Toc101359996)

[**2.1.** **METIS Access** 8](#_Toc101359998)

[**2.2.** **EMEA-CIB\UTXXX\_A Admin user** 8](#_Toc101359999)

[**2.3.** **ASIA-CIB\UTXXX\_A Admin user** 9](#_Toc101360000)

[**2.4.** **London Domain Accounts (Domain : LDN)** 9](#_Toc101360001)

[**2.5.** **CyberArk SAFES** 10](#_Toc101360002)

[**2.6.** **IPANEMA/SALSA Access** 10](#_Toc101360003)

[**2.7.** **Skype Instant Messaging** 10](#_Toc101360004)

[**2.8.** **IOBEYA (White Board)** 11](#_Toc101360005)

[**2.9.** **LPM Domain accounts (Domain: AF-CIB)** 11](#_Toc101360006)

[**2.10.** **LPM – Secured Bastion** 11](#_Toc101360007)

[**2.11.** **All Other Security access** 11](#_Toc101360008)

[**3.** **METIS Habilitation** 12](#_Toc101360009)

[**3.1.** **Shared mailboxes (Network & Security Operations / network-security-operations)** 13](#_Toc101360011)

[**3.2.** **EMEA-CIB\UTXXXX Normal User** 13](#_Toc101360012)

[**3.3.** **Citrix access** 13](#_Toc101360013)

[**3.4.** **Sharepoint Document Repositories** 13](#_Toc101360014)

[**3.5.** **METIS Functional management group** 14](#_Toc101360015)

[**3.6.** **Network Device Access via TACACS** 14](#_Toc101360016)

[**3.7.** **HP Network Automation** 14](#_Toc101360017)

[**3.8.**  **HP NNM** 14](#_Toc101360022)

[**3.9.** **Shared Folder Access** 15](#_Toc101360023)

[**4.** **CyberArk** 15](#_Toc101360024)

[5. Citrix 18](#_Toc101360025)

[6. Inventory and diagrams 18](#_Toc101360026)

[**6.1.** Sharepoint directories 18](#_Toc101360030)

[**6.2.** IP Addresses (Infoblox) 19](#_Toc101360031)

[**6.3.** SEC Inventory and NSO KeePass 19](#_Toc101360032)

[**6.4.** PMEP Checker 19](#_Toc101360033)

[**6.5.** COMITS – CHG and INC communication 20](#_Toc101360034)

[**6.6.** HP NNM Monitoring 20](#_Toc101360035)

[**6.7.** Qradar and Algosec 20](#_Toc101360036)

[**6.8.** Cacti and Splunk 20](#_Toc101360037)

[**6.9.** ESTEL-IBM Inventory process 20](#_Toc101360038)

[**6.10.** Network Security Operations (NSO) WIKI 21](#_Toc101360039)

[7. EMEA Infrastructure – network & security devices access 21](#_Toc101360040)

[**7.1.** Network devices 21](#_Toc101360042)

[Arista Switches 21](#_Toc101360043)

[Juniper EX4200 Switches 21](#_Toc101360044)

[**7.2.** Cisco APIC 21](#_Toc101360045)

[**7.3.** IPANEMA 22](#_Toc101360046)

[**7.4.** Juniper Netscreen- ISG 1000 22](#_Toc101360047)

[ADS-T VPN Concentrator 22](#_Toc101360048)

[SGA 22](#_Toc101360049)

[**7.5.** Juniper SRX 23](#_Toc101360050)

[**7.6.** Checkpoint ADS-I 23](#_Toc101360051)

[MGMT console 23](#_Toc101360052)

[Mutli-Domain Server and GWs 24](#_Toc101360053)

[**7.7.** Fortigate 24](#_Toc101360054)

[FortiManager 24](#_Toc101360055)

[FortiAnalyser 24](#_Toc101360056)

[**7.8.** BIG IP F5 24](#_Toc101360057)

[**7.9.** Proxy McAfee 25](#_Toc101360058)

[**7.10.** Pulse Secure 26](#_Toc101360059)

[**7.11.** IPS TippingPoint 26](#_Toc101360060)

[**7.12.** Strong Authentication AAA 27](#_Toc101360061)

[8. ASIA Infrastructure – network & security devices access 27](#_Toc101360062)

[**8.1.** GRANT Requests 27](#_Toc101360064)

[**8.2.** Network devices 28](#_Toc101360065)

[**8.3.** Fortinet Ascenlink 29](#_Toc101360066)

[**8.4.** Cisco ISE 29](#_Toc101360067)

[**8.5.** Cisco WLC 29](#_Toc101360068)

[**8.6.** Fortinet 29](#_Toc101360069)

[**8.7.** Checkpoint 30](#_Toc101360070)

[Gateways 30](#_Toc101360071)

[Management Console 30](#_Toc101360072)

[**8.8.** Juniper SSG 31](#_Toc101360073)

[**8.9.** BIG IP F5 31](#_Toc101360074)

[Internal & DR 31](#_Toc101360075)

[DMZ 32](#_Toc101360076)

[**8.10.** Pulse Secure 32](#_Toc101360077)

[**8.11.** Proxy McAfee 32](#_Toc101360078)

[**8.12.** IPS TippingPoint 33](#_Toc101360079)

[**8.13.** AAA Active Identity 33](#_Toc101360080)

[**8.14.** MRTG/CACTI 33](#_Toc101360081)

[**8.15.** PAC file Folder 34](#_Toc101360082)

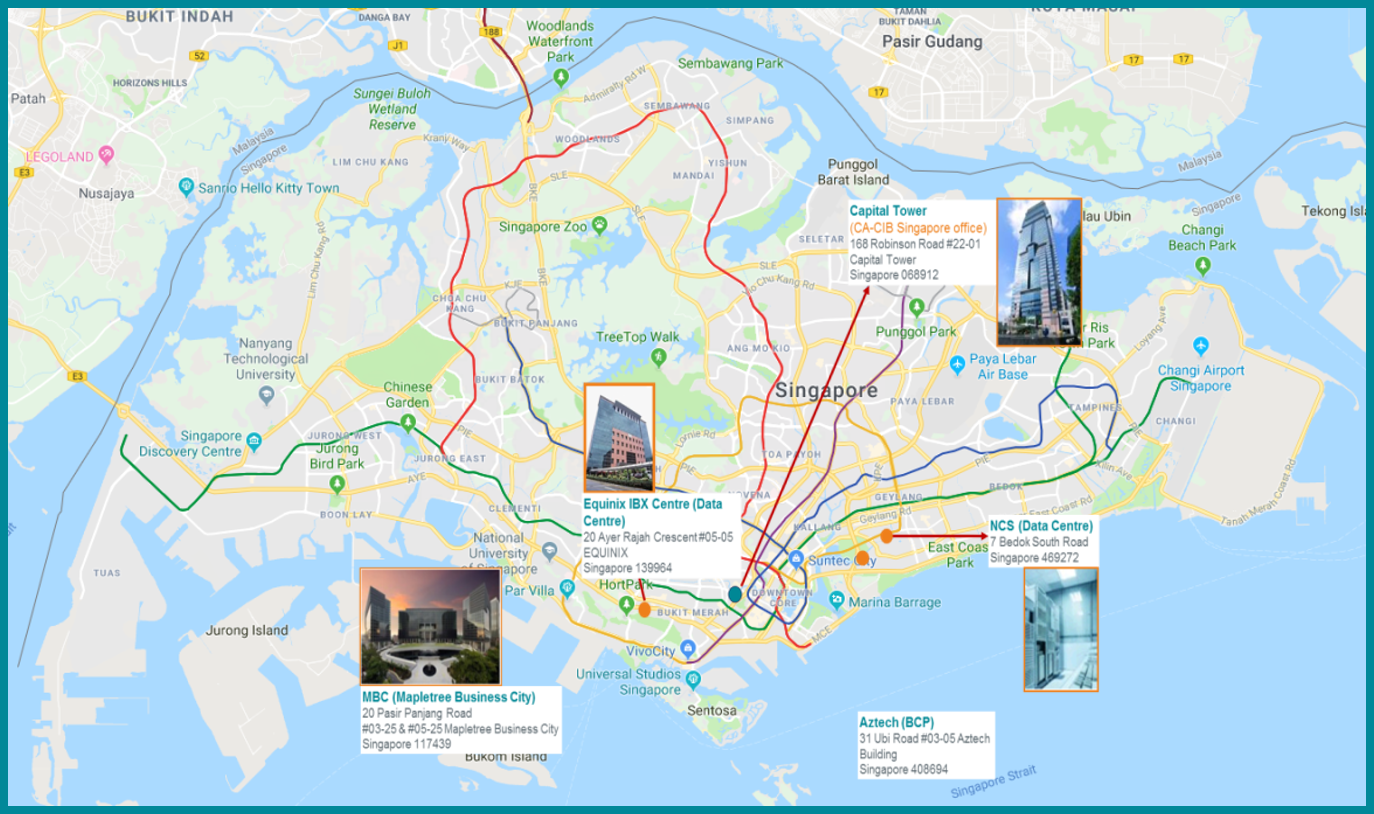
[**8.16.** Asia Active Directory 34](#_Toc101360083)

# **Administrative**

## Office access

ISAP offices are mainly located in Mapletree Business City, segregated in two different buildings, the 20 (3rd , 5th and 6th floors) and 80 Pasir Panjang Road (23rd Floor)  
NSO team is sitting in MBC20 5th floor, seats W172 to W192 highlighted below ([MBC20 FloorPlan](http://portal.isap.asia.cib/News/Documents/5F%20MBC%20WS%20by%20name_2018-12.pdf))





## CA-CIB and WIPRO attendance

CACIB Attendance : <http://diana.ca.cib/>

WIPRO attendance : <http://git.ca.cib/collab/aps-prod/CIS/nss/Public%20Documents/Forms/AllItems.aspx?RootFolder=%2Fcollab%2Faps%2Dprod%2FCIS%2Fnss%2FPublic%20Documents%2FSA2%20Shift%20Planning&FolderCTID=0x01200094CDA55E4AABC34DB07C214C2AFBB32F&View=%7bBB545FFF-2DE3-4F75-9B50-5C9B509E8AC0%7d>

## eLearning

Under 24 hours, all new joiners have to complete mandatory [**CA-CIB e-Learning URL**](http://ca-cib.elearning.ca-ifcam.fr/)You should have received an email regarding training to complete, otherwise please check in “My current course” part of the e-Learning portal

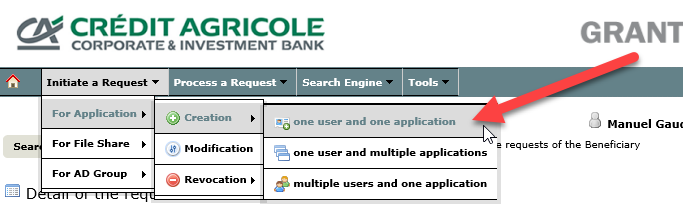
# **GRANT Habilitation**

Access to applications, equipment, Data Center are all granted to your UT code using [GRANT](http://arm.cm.par.emea.cib/arm/grantflow.html?_flowId=basic-flow) application

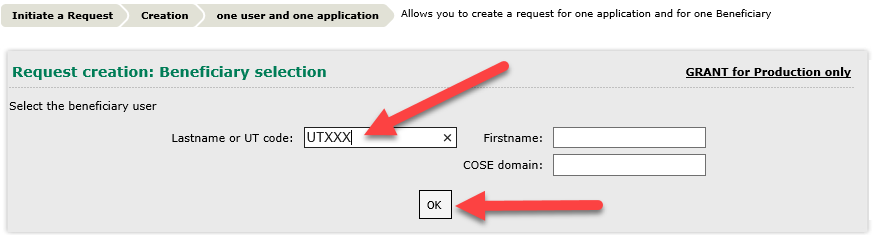
Active Directory user convention is called UT code (ex. UTxxx) in following domains :  
- ASIA-CIB for Asia (also called ISAP)  
- EMEA-CIB for all Europe countries  
- LDN-CIB for UK

User accounts can be of multiple formats :  
- UTxxx : Normal User  
- UTxxx\_A : Administrator Account  
- UTxxx\_SO : System Operator Account

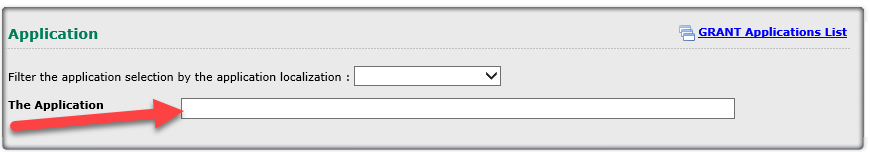
[GRANT](http://arm.cm.par.emea.cib/arm/grantflow.html?_flowId=basic-flow) tool is used for requesting access  
Click on Initiate a Request / For Application / Creation / one user and one application



Type your UT code and click OK



Next screen with let you select which application you want to access (use application code)





## **METIS Access**

Application code : **METIS**  
Application Name : METIS  
Validation Path : METIS specific profiles validation

Profile: ADMIN  
Specify your need: New joiner and need access to support daily operations.

## **EMEA-CIB\UTXXX\_A Admin user**

“Jump Servers” are used for accessing admin interfaces of Network and Security equipment.  
These servers are part of EMEA-CIB domain and require an admin account to connect

Application code : **1PADPAR**  
Application Name : Privileged Active Directory Accounts - EMEA domain  
Validation Path: EMEA UTxxxx\_A, \_DA, \_EA, \_O or\_SO AD account

Profile: Administrator  
Description : Server Adm (UTXXX\_A)

Specify your need: New joiner in NSO team. Need rights for daily administration.

Please add the below groups in the account EMEA-CIB\UT2XXX\_A :  
EMEA-CIB\Domain Users  
EMEA-CIB\NSS-SEC

For Security use:

-----------------------  
EMEA-CIB\UADM\_CA\_SF\_AE\_FORTIGATE\_ADMIN\_ADMIN  
EMEA-CIB\UADM\_CA\_SF\_AE\_TRENDMICRO\_IPS\_ADMIN\_ADM  
EMEA-CIB\U\_ISILON\_AV\_PRD  
EMEA-CIB\UADM\_CA\_SF\_ASIA\_FORTIGATE\_REC\_ADM  
EMEA-CIB\UADM\_CA\_SF\_ASIA\_TRENDMICRO\_IPS\_REC\_ADM  
EMEA-CIB\UADM\_CA\_SF\_AT\_FORTIGATE\_ADM   
EMEA-CIB\UADM\_CA\_SF\_AU\_TRENDMICRO\_IPS\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_BE\_TRENDMICRO\_IPS\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_CA\_TRENDMICRO\_IPS\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_CH\_TRENDMICRO\_IPS\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_CN\_TRENDMICRO\_IPS\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_DE\_FORTIGATE\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_DE\_TRENDMICRO\_IPS\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_ACTIVEIDENTITY\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_ALGOSEC\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_AUTHENT\_ADMIN\_MGR   
EMEA-CIB\UADM\_CA\_SF\_AUTHENTREC\_ADMIN\_MGR   
EMEA-CIB\UADM\_CA\_SF\_FR\_CHECKPOINT\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_CHECKPOINT\_EXPERT\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_CHECKPOINT\_MGT\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_F5\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_F5\_REC\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_FIREW\_ADMIN\_MGR   
EMEA-CIB\UADM\_CA\_SF\_FR\_FIREWREC\_ADMIN\_MGR   
EMEA-CIB\UADM\_CA\_SF\_FR\_FORTIANALYZER\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_FORTIGATE\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_FORTIGATE\_REC\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_FORTIMANAGER\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_FR\_JUNIPER\_ADMIN\_ADM   
EMEA-CIB\UADM\_CA\_SF\_SG\_ALGOSEC\_ADMIN\_ADM

**To Access PARGUI:**

Once this request is validated, verify connection via Remote Desktop Connection (mstsc.exe) using EMEA-CIB\UTXXX\_A :

|  |  |
| --- | --- |
| PARGUI1 (CMSUPA023) | 10.126.254.14 |
| PARGUI2 (CMSUPA024) | 10.126.254.34 |
| PARGUI3 (CMSUPA074) | 10.126.254.18 |

## **ASIA-CIB\UTXXX\_A Admin user**

“Jump Servers” are used for accessing admin interfaces of Network and Security equipment.  
These servers are part of EMEA-CIB domain and require an admin account to connect

Application code : **1PADASIA**  
Application Name : Privileged Active Directory Accounts - ASIA domain  
Validation Path: ASIA.CIB AD account for OPUS users

Profile: Administrator  
Description : Server Adm (UTXXX\_A)

Specify your need: New joiner in NSO team. Need rights for daily administration.

## **ISAP Network Devices**

Whoever wants to access network devices must have approved grant for ISAP Network Devices and added the UTCODE\_A in AD GROUP (UADM\_NET\_ISAP\_ADMINS) assigned for network.

Application code: **1NDISAP**

Validation Path: ISAP Network Devices

Profile: Administrator

Justification: Need access to support daily operations.

Specify your needs: Please add ASIA-CIB\UTCODE\_A in AD GROUP (UADM\_NET\_ISAP\_ADMINS)

Once above are settled he/she needs to use Jump Server below to access/login all network devices.

10.147.100.246

10.147.100.247

## **ISAP Firewall Admin Rights**

Whoever wants to access ISAP security devices must have approved grant for ISAP Network Devices and added the UTCODE\_A in AD GROUP (UADM\_NET\_ISAP\_ADMINS) assigned for network.

Application code: **1FWISP**

Application Name: ISAP firewall administration rights

Validation Path: ISAP Infrastructure - Firewall Administration Rights

Profile: Administrator

Justification: Firewall access to ISAP Security Devices as part of BAU for NSO

Specify your needs: Firewall access to ISAP Security Devices as part of BAU for NSO

## **London Domain Accounts (Domain : LDN)**

There are two account need to be created for London one is normal account (UTXXXX) with internet access and another one (UTXXXX\_A) is for administrative purpose.

Application code : **ADLDN**  
Application Name: ACTIVE DIRECTORY (LDN DOMAIN)

Validation Path: A Personal London Network & Email Account

Specify your need: New joiner in NSO team. Need rights for daily administration.

* Normal domain account with internet and citrix access: sample account – UT2F83
* UTXXXX\_A account: sample account UT2F83\_A

UTXXXX\_A Account to be added to below AD groups:

AS\_Infrastructure Security Administration\_G

DL\_UK\_ISILON\_AV

**Justification:** Newly joined in Network security operations team and need to have below access to support London network security operations.

## **Device42**

Application code : **GBRD42**  
Application Name : DEVICE42 GBR  
Validation Path: Device42 GBR access

Profile: Read/Write  
Description : Read/Write

Specify your need: New joiner in NSO team. Need rights for daily administration.

## **CyberArk SAFES**

Application code : **1CILPAR**  
Application name: Infrastructure - CISCO ISE LAN EMEA

Validation Path : Infrastructure - CISCO ISE LAN EMEA

Profile : EMEA SAFE administrator

## **IPANEMA/SALSA Access**

Application code : **1IPNPAR**  
Application Name : Infrastructure - Ipanema  
Validation Path: Infrastructure-Ipanema  
Profile: SAFE Administrator  
Fill all other required details

Application code : **1SAPAR**  
Application Name : Infrastructure - Salsa  
Validation Path: Infrastructure-Salsa  
Profile: Paris SAFE Administrator  
Fill all other required details

## **Skype Instant Messaging**

Application code: **SKYPE**

Application Name: SKYPE FOR BUSINESS

Validation Path: SKYPE Standard for SINGAPORE Opus Users

Click on Form to fill and attach under Attached File

## **IOBEYA (White Board)**

Application code: **IOBEYA**

Application Name: IOBEYA (IOBEYA)

Validation Path: IOBEYA\_Access

Profile: IOBEYA\_RoomMaster

Specify your need: Kindly assist to grant access to the room "ISAP ITS NSS".

## **LPM Domain accounts (Domain: AF-CIB)**

Application code: **AD2SR**

Application Name: ACTIVE DIRECTORY 2SR

Validation Path: 2SR AD – ITS – Admin Account

Profile: 2SR AD Admin Account

Description: 2SR AD Admin Account (UTXXXX\_A)

## **LPM – Secured Bastion**

|  |  |
| --- | --- |
| **APPLICATION** | **GRANT Application Name** |
| ***ACTIVE DIRECTORY*** | **AD2SR – ACTIVE DIRECTORY 2SR** |
| *(création de comptes UT\_A)* |
| ***ALGOSEC*** | **BSALGO - ALGOSEC 2SR** |
| ***ALTIRIS*** | **BSALT - ALTIRIS 2SR** |
| ***GPP*** | **BSGPP - GPP 2SR** |
| ***EXACC*** | **BSECC - EXACC 2SR** |
| ***F5*** | **BSF5 - F5 2SR** |
| ***FIREWALL*** | **BSFRWL - FIREWALL 2SR** |
| ***SQL*** | **BSSQL - SQL 2SR** |
| ***PRIZE ADMIN*** | **BSPA - PRIZE ADMIN 2SR** |
| ***MQ*** | **BSMQ - MQ 2SR** |
| ***ONEVIEW*** | **BSOV - ONEVIEW 2SR** |
| ***PKI*** | **BSPKI - PKI 2SR** |
| ***PostgreSQL*** | **BSPSQL - PostgreSQL 2SR** |
| ***SEP*** | **BSSEP - SEP 2SR** |
| ***SWITCH*** | **BSSWIT - SWITCH 2SR** |
| ***UNIX*** | **BSUNX - UNIX 2SR** |
| ***WINDOWS*** | **BSWIN - WINDOWS 2SR** |
| ***PULSE (remote access)*** | **PLS2SR - Remote connection - 2SR** |

## **All Other Security access**

Application Derogation for Internet standard access (1DISPAR)

Application Infrastructure - McAfee Gateway Paris (1MAPAR) Remote access SuperAdmin

Application Infrastructure - Juniper EMEA (1JUPAR)

Application Infrastructure - Firewall LDN (1FIRLDN)

Application Infrastructure - Actividentity Paris (1AIDPAR)

Application ALGOSEC SUITE (ALGSEC)

Application Infrastructure - Fortigate EMEA (1FGEPAR)

Application Infrastructure - Fortianalyser Admin Tools ISAP (1FATISAP)

Application Infrastructure - SMS Paris (1SMSPAR)

Application Infrastructure - IPS EMEA (1IPSEMEA)

Application Infrastructure - IPS Asia (1IPSASI)

Application Infrastructure - IPS America (1IPSUS)

Application Infrastructure - Checkpoint EMEA (1CPPAR)

Application QRADAR (QRAD)

Application Infrastructure - Fortimanager EMEA (1FTEMEA)

Application MOVIS (MOVIS)

Application SUNGARD MAL GBR (SMAL)

Application Infrastructure - F5 Paris (1F5PAR)

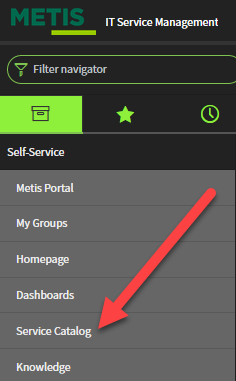
Application Infrastructure - F5 Russia (1F5RUS)

Application DROP (DRP)

# **METIS Habilitation**

METIS is CA-CIB ticketing system for Request, Changes and Incidents.  
URL is <https://cagip.service-now.com/>

Snowboard is also used for extracting reports : <https://snowboard.emea.cib/>

Access requests can be requested via top left menu Self Service - Service Catalog  




## **Shared mailboxes (Network & Security Operations / network-security-operations)**

*Service Catalog >> Catalog CACIB >> Office – SG - CACIB >>SG Messaging (Outlook, Reuters) >> SG Generic Mailbox : Create / Modify / Delete*

* + Location: Requestor’s Location
  + Project code: Run
  + Request Type: Generic Mailbox: Modify
  + Mailbox name: network-security-operations
  + Modification Type: Modify Full Mailbox permission
  + Action – Add members
  + Which Members to add or remove – Select the members

**NOTE:** After the request, if you still have access issues to common mailboxes (sending & receiving emails) please open a request to messaging team to grant access.

## **EMEA-CIB\UTXXXX Normal User**

*Service Catalog >> Catalog CACIB >> Office – FR - CACIB >> Authorization management (except Grant) and files management >> AD Account : Enable/Close*

AD account name: EMEA-CIB\UTXXXX

Comments: Add new member to EMEA AD group to support daily operations.

## **Citrix access**

*Service Catalog >> Catalog CACIB >> Office – FR - CACIB >> Applications and Softwares >> Citrix Icons: Install / Remove*

*Service Catalog >> Catalog CACIB >> Office – SG - CACIB >> SG Applications and software >> SG Citrix: Administration*

**\*Request Type**: Add

In list of software select any random application and update requirement in description and mention your team name like (SA02\01). Habilitations team will process the ticket.

## **Sharepoint Document Repositories**

*Service catalog >> Catalog CACIB >> Office – SG - CACIB >> SG Applications and software >> SG SharePoint Request*

Provide your UT code and request access to following Sharepoint websites :

**NSS Portal**  
http://git.ca.cib/collab/aps-prod/CIS/nss/SitePages/Home.aspx

**ISAP Portal**<https://ca-cib.ca-mocca.com/sgp/GIT-ITS-NSO/SitePages/Home.aspx>

## **METIS Functional management group**

*Service Catalog >> Catalog CAGIP >> Production CAGIP >> Catalogue de Service METIS >> METIS : Functional management of a group*

**\*Short description**: Add member to Group.

**\*Group name:** (One request for one group)

CAGIP-GRC-Metis-SACM-Writer

CAGIP-GRC-TELECOM-NETWORK-SECURITY-OPS-SUP-IT-GL-L1L2

CAGIP-GRC-CHG\_A-ROUTINE-FR-CAB

CAGIP-GRC-CHG\_A-EMERGENCY-FR-CAB

CAGIP-GRC-TELECOM-NETWORK-ALERT-SUP-IT-GL-L1

**\*Options:** Adding member(s) to the group

**\*Available member(s) to the group:**

>> Search and select new joiner name to the right box.

## **Network Device Access via TACACS**

*Service Catalog >> Catalog CACIB >> Office – FR – CACIB >> Authorization management (except Grant) and files management >> Authorization out of GRANT: Create / Revoke*  
Ask the Habilitations team to add your AD EMEA and ASIA account in **DL\_TACACS\_PAR\_ACS** (If you need only RO access please mention the group name as DL\_TACACS\_PAR\_NSS\_RO and note that this will also deny the user from executing show running-config on Nexus platforms)

## **HP Network Automation**



*Service Catalog >> Catalog CACIB >> Production CACIB >> Infrastructure Services >> Network >> Network Management >> Other Network Request*

Mention that you need access to PARNA3/PARN4

PARNA3 and PARNA4 are HPNA servers, for configuration backup and automation  
Access via <https://parna3.par.emea.cib> and <https://parna4.par.emea.cib> using UT code

## **3.8. HP NNM**

*Service Catalog >> Catalog CACIB >> Office – FR – CACIB >> Authorization management (except Grant) and files management >> Authorization out of GRANT: Create / Revoke*

Request Habilitation team to add UT code to DL\_NNM\_OPERATOR-L2\_PRD AD group in comment  
NOTE : Manager approval is mandatory

## **Shared Folder Access**

*Service Catalog >> Catalog CACIB >> Office – FR – CACIB >> Authorization management (except Grant) and files management Existing shared folder : Request permission*

\***Access type:** Read-Write Access

\***Full path to the share directory (**[**\\server\_name\directory**](file:///\\server_name\directory)**)**

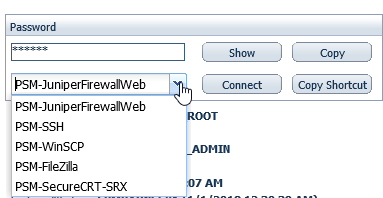
[\\cmfrfi002.cm.par.emea.cib\Reseaux\_securite](file:///\\cmfrfi002.cm.par.emea.cib\Reseaux_securite)

# **CyberArk**

Password vault for admin account

URL is <https://pvw.emea.cib/> with following credential :  
login : [UTxxx\_A@emea.cib](mailto:UTxxx_A@emea.cib)  
password: <\_A password>

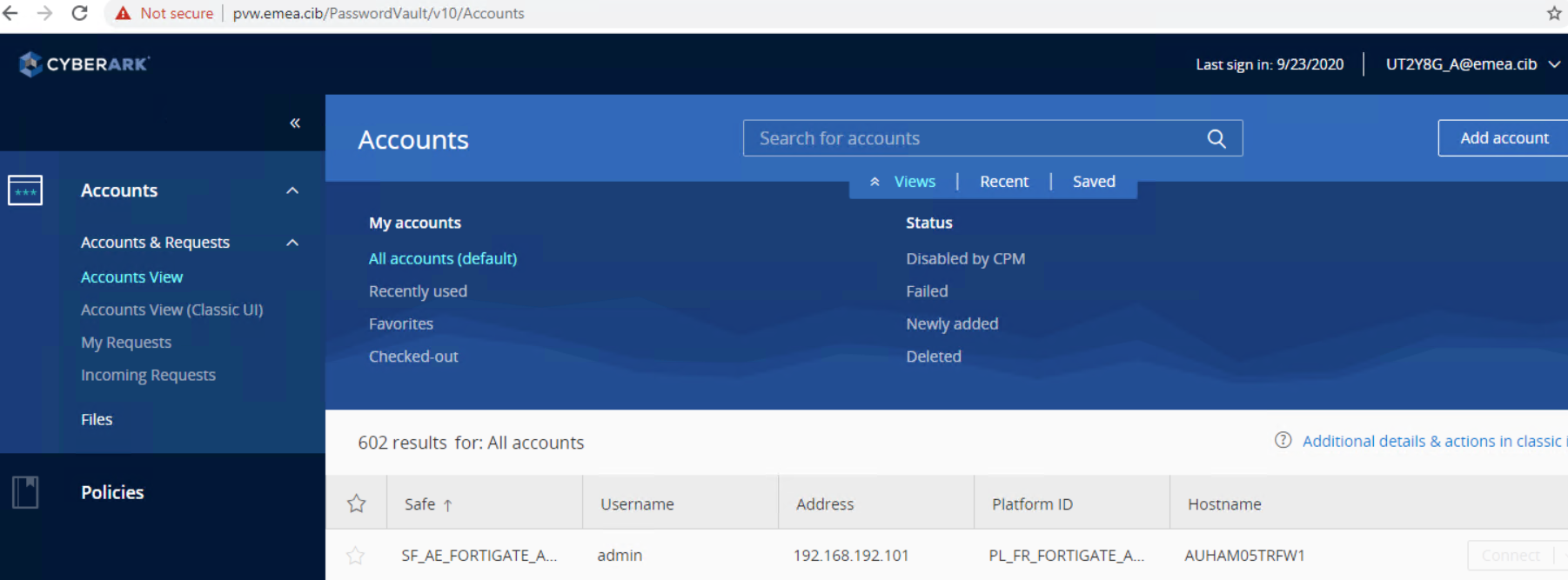
Type equipment name in the search bar to find related account

You will have the choice to reveal, copy password or even connect to the equipment using a jump server if configured

Access Control is done via Safes :

|  |
| --- |
| SF\_AE\_FORTIGATE\_ADMIN |
| SF\_AE\_TRENDMICRO\_IPS\_ADMIN |
| SF\_AR\_TRENDMICRO\_IPS\_ADMIN |
| SF\_ASIA\_FORTIGATE\_REC |
| SF\_ASIA\_TRENDMICRO\_IPS\_REC |
| SF\_AT\_FORTIGATE\_ADMIN |
| SF\_AU\_TRENDMICRO\_IPS\_ADMIN |
| SF\_BE\_TRENDMICRO\_IPS\_ADMIN |
| SF\_BR\_TRENDMICRO\_IPS\_ADMIN |
| SF\_CA\_TRENDMICRO\_IPS\_ADMIN |
| SF\_CH\_TRENDMICRO\_IPS\_ADMIN |
| SF\_CN\_TRENDMICRO\_IPS\_ADMIN |
| SF\_DE\_FORTIGATE\_ADMIN |
| SF\_DE\_TRENDMICRO\_IPS\_ADMIN |
| SF\_DZ\_FORTIGATE\_ADMIN |
| SF\_DZ\_TRENDMICRO\_IPS\_ADMIN |
| SF\_ES\_JUNIPER\_ADMIN |
| SF\_ES\_TRENDMICRO\_IPS\_ADMIN |
| SF\_FR\_ACTIVEIDENTITY\_ADMIN |
| SF\_FR\_ALGOSEC\_ADMIN |
| SF\_FR\_AUTHENT\_ADMIN |
| SF\_FR\_AUTHENTREC\_ADMIN |
| SF\_FR\_CHECKPOINT\_ADMIN |
| SF\_FR\_CHECKPOINT\_EXPERT |
| SF\_FR\_CHECKPOINT\_MGT\_ADMIN |
| SF\_FR\_CISCOISE\_LAN\_ADMIN |
| SF\_FR\_CISCOISE\_REC |
| SF\_FR\_F5\_ADMIN |
| SF\_FR\_F5\_REC |
| SF\_FR\_FIREW\_ADMIN |
| SF\_FR\_FIREWREC\_ADMIN |
| SF\_FR\_FORTIANALYSER\_ADMIN |
| SF\_FR\_FORTIGATE\_ADMIN |
| SF\_FR\_FORTIGATE\_REC |
| SF\_FR\_FORTIMANAGER\_ADMIN |
| SF\_FR\_JUNIPER\_ADMIN |
| SF\_FR\_JUNIPER\_NSM\_ADMIN |
| SF\_FR\_JUNIPER\_REC |
| SF\_FR\_MCAFEE\_ADMIN |
| SF\_FR\_MCAFEE\_EPO\_ADMIN |
| SF\_FR\_MONIT\_ADMIN |
| SF\_FR\_MONITREC\_ADMIN |
| SF\_FR\_PROXY\_ADMIN |
| SF\_FR\_PROXYREC\_ADMIN |
| SF\_FR\_REMOTEA\_ADMIN |
| SF\_FR\_REMOTEAREC\_ADMIN |
| SF\_FR\_RP-LB\_ADMIN |
| SF\_FR\_RP-LBREC\_ADMIN |
| SF\_FR\_SEC\_SERVICE |
| SF\_FR\_SMS\_TIPPING\_ADMIN |
| SF\_FR\_TRENDMICRO\_IPS\_ADMIN |
| SF\_FR\_TRENDMICRO\_IPS\_REC |
| SF\_HK\_TRENDMICRO\_IPS\_ADMIN |
| SF\_IN\_FORTIGATE\_ADMIN |
| SF\_IN\_TRENDMICRO\_IPS\_ADMIN |
| SF\_IT\_JUNIPER\_ADMIN |
| SF\_IT\_TRENDMICRO\_IPS\_ADMIN |
| SF\_JP\_TRENDMICRO\_IPS\_ADMIN |
| SF\_KR\_TRENDMICRO\_IPS\_ADMIN |
| SF\_MX\_TRENDMICRO\_IPS\_ADMIN |
| SF\_NL\_FORTIGATE\_ADMIN |
| SF\_RU\_CHECKPOINT\_ADMIN |
| SF\_RU\_CHECKPOINT\_EXPERT |
| SF\_RU\_CHECKPOINT\_MGT\_ADMIN |
| SF\_RU\_FORTIGATE\_ADMIN |
| SF\_RU\_JUNIPER\_ADMIN |
| SF\_RU\_TRENDMICRO\_IPS\_ADMIN |
| SF\_SA\_FORTIGATE\_ADMIN |
| SF\_SE\_FORTIGATE\_ADMIN |
| SF\_SE\_TRENDMICRO\_IPS\_ADMIN |
| SF\_SG\_ALGOSEC\_ADMIN |
| SF\_SG\_TRENDMICRO\_IPS\_ADMIN |
| SF\_US\_ALGOSEC\_ADMIN |
| SF\_US\_TRENDMICRO\_IPS\_ADMIN |
| SF\_US\_TRENDMICRO\_IPS\_REC |

*/!\ it is recommended to use Chrome when using CyberArk and to switch to the new view.*



# Citrix

<https://myapps.emea.cib/Citrix/MyAccessWeb/>  -- Paris Citrix  
<http://myxenapp.ldn.emea.cib/Citrix/XenApp/site/default.aspx>  -- London Citrix  
<https://mycitrixapps.isap.asia.cib/Citrix/MyAppsISAPWeb> -- ISAP Citrix

# Inventory and diagrams



## Sharepoint directories

[**NSS Portal**](http://git.ca.cib/collab/aps-prod/CIS/nss/SitePages/Home.aspx) : Main team portal (NSS-ISAP)   
Most diagrams are located at following URL : <http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/Forms/AllItems.aspx?RootFolder=%2Fcollab%2Faps%2Dprod%2FCIS%2Fnss%2FPrivate%20Documents%2FNSO>

Most important diagrams are :  
MAN: <http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/PARIS/MAN/Diagram/SCH_MAN-MPLS-v3-propo.vsd>

WAN: [http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/WAN/Diagrams/SCH\_WAN\_v14.0.vsd](http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/WAN/Diagrams/Old/SCH_WAN_v14.0.vsd)

DC + ACI: [http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/PARIS/DATACENTER/Diagrams/LAN%20DC%20OVERVIEW.VSD](http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/PARIS/DATACENTER/Diagrams/_OLD_/LAN%20DC%20OVERVIEW.VSD)

ADSL: <http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/Forms/AllItems.aspx?RootFolder=%2Fcollab%2Faps%2Dprod%2FCIS%2Fnss%2FPrivate%20Documents%2FNSO%2FPARIS%2FADSL%2FDiagrams>

ADSI: <http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/ADS-i%20WorldWide/ADS-i%20FRANCE%20(Paris)/SCH_Global_ADSI.vsd>

Most important documents are :

ADS-I engineering : <http://git.ca.cib/collab/aps-prod/CIS/nss/Public%20Documents/Standards_Documents/ADS-i/Standard%20-%20ADSI%20security%20services%20v7.3.pdf>

Device naming convention : <http://git.ca.cib/collab/aps-prod/CIS/nss/Public%20Documents/Standards_Documents/Naming_convention_Devices/Security%20devices%20naming%20convention%20v1_4.pdf>

**ISAP Portal :**   
https://ca-cib.ca-mocca.com/sgp/GIT-ITS-NSO/SitePages/Home.aspx

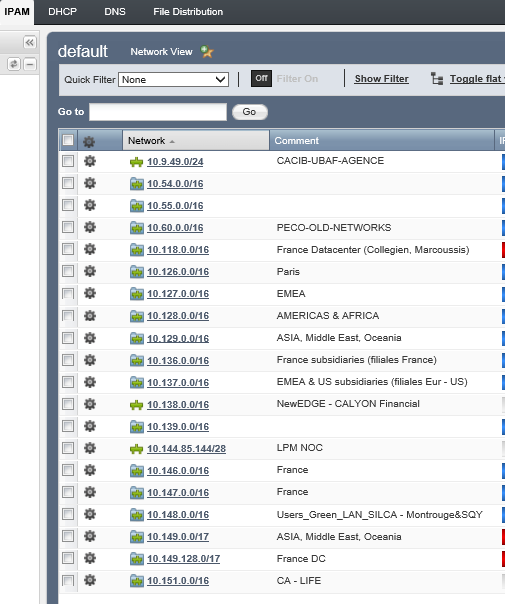
Open a service request on the below path in ServiceNow and provide your UT code (Providing a reference UT code will speed up the request)  
*Service Catalog > Application Services > Support > Access > Middleware Access > SHAREPOINT*

**NOTE:** After the request, if you need to speed it up after raise you can contact hamed Khaleel or Roel Dancel

## IP Addresses (Infoblox)

<https://ipam.ca.cib> – Infoblox IPAM (DHCP and DNS) – Use EMEA-CIB\UTxxx\_A account

<http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/ADS-i%20WorldWide/ADS-i%20FRANCE%20(Paris)/DMZ%20IP%20Assignment>  -- DMZ IP assignment



## SEC Inventory and NSO KeePass

Inventory for all security devices is stored in [Sharepoint SEC ACT Inventory\_NSS folder](http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/Forms/AllItems.aspx?RootFolder=%2Fcollab%2Faps%2Dprod%2FCIS%2Fnss%2FPrivate%20Documents%2FNSO%2F%5FGlobal%20infrastructure%20or%20service%2FInventory)  
This document is password-protected

Keepass application is installed in all CA-CIB workstations/laptops masters.  
It is used to store equipment password, it is stored in [NSO Keepass file](http://git.ca.cib/collab/aps-prod/CIS/nss/Private%20Documents/NSO/NSO.kdbx)

## PMEP Checker

Website used to present all possible actions and impact/severity of all changes in infrastructure  
<http://apsprod.par.emea.cib/pmepchecker/index.php?page=pmep-infra&action=filters&filt_1=NSS&ldT_1=domain>

## COMITS – CHG and INC communication

<http://comits-new.par.emea.cib/>  
Email communication before and after a change activity, and/or during incident

## HP NNM Monitoring

<https://nnmparprd.emea.cib/nnm/>

Used by Global Operation Center (GOC) to open Incidents tickets and assign to our queue

## Qradar and Algosec

<https://10.147.111.7> – Qradar used for IPS alerting and logs  
<https://10.126.254.30/algosec/suite/login.html>  -- Algosec for firewall rules analysis

## Cacti and Splunk

Cacti v0.8.7 Asia with WeatherMap: <http://asiamrtg.isap.asia.cib/> (use UTxxx account)  
Cacti v0.8.7 Paris : <http://cacti.par.emea.cib/cacti/graph_view.php?action=tree&tree_id=33&leaf_id=919&select_first=true>  
Cacti v1.1.38 Paris with WeatherMap : <http://cmvp06ca.prd.cm.par.emea.cib:8080/cacti/index.php>

Splunk : <http://10.179.0.97:8000/en-US/account/login?return_to=%2Fen-US%2F#en-US/account/login?return_to=%2Fen-US%2F> (use UTxxx account)

## ESTEL-IBM Inventory process

To update/create/modify IBM Inventory for maintenance,

* please download the spreadsheet “ESTEL – Request update inventory template v2.xslx” located at <https://ibm.box.com/v/Box-Partage-Contrat-Estel>

CREDIT AGRICOLE – IBM : ESTEL  
DOCUMENTS & PROCEDURES TOUTES ENTITES  
INVENTAIRES

* Send the completed spreadsheet to following email addresses :  
  [marc.buisine@fr.ibm.com](mailto:marc.buisine@fr.ibm.com)  
  [bernard.demeure@fr.ibm.com](mailto:bernard.demeure@fr.ibm.com)  
  cc : [philippe.talbot@fr.ibm.com](mailto:philippe.talbot@fr.ibm.com)
* IBM validates requested modification
* If modification validated, IBM creates a commercial contract
* Commercial contract sent to CA-CIB
* CA-CIB validates commercial contract by sending email agreement
* IBM adds new equipment under maintenance within one month after commercial agreement reception

## Network Security Operations (NSO) WIKI

All the network security process and information can be found here

[\\Cmfrfi002\Reseaux\_Securite\Etudes & Productions - Réseaux & Securité\NSOWIKI](file://Cmfrfi002/Reseaux_Securite/Etudes%20&%20Productions%20-%20Réseaux%20&%20Securité/NSOWIKI)  
Open as OneNote document

# EMEA Infrastructure – network & security devices access



## Network devices

*/!\Please do not modify any configuration when connected to the below switches.*

### Arista Switches

Use MobaXterm on PARGUI2 to ssh CLIVN1LF1W2 10.146.86.134.

### Juniper EX4200 Switches

*/!\Cannot access these switches directly from PARGUI*

Ssh from PARNA3/4 CY01VNW2 10.146.80.18.

Cisco Nexus7000

Use MobaXterm on PARGUI2 to ssh CY03VNT5 10.149.138.20

## Cisco APIC

Use FireFox on PARGUI2 10.126.254.34. Use normal UTXXXX code.

<https://10.149.131.11>

## IPANEMA

Use FireFox on PARGUI2 10.126.254.34.

*/!\ ask EMEA network admin to create a local UT account.*

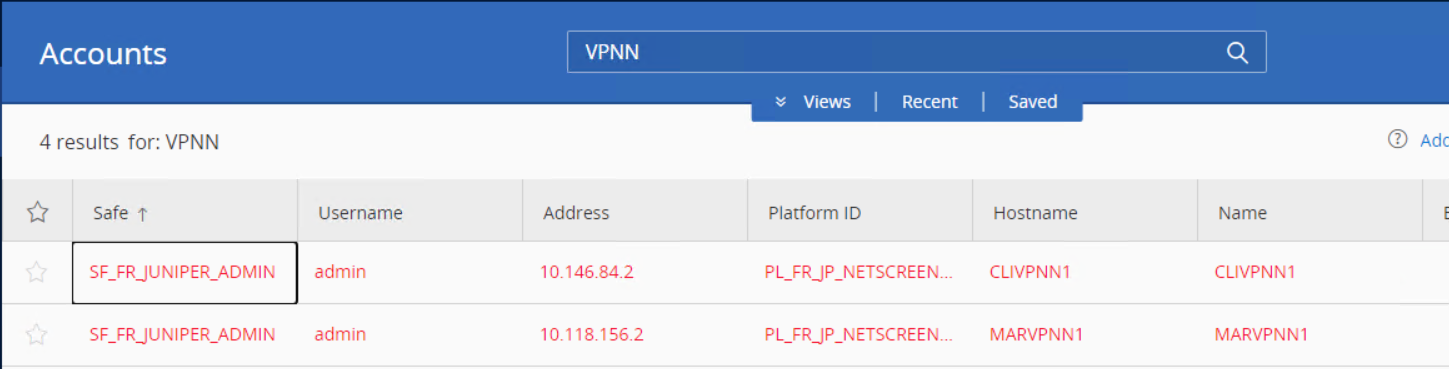
<https://wpvpaap0000gzzs.emea.cib/salsa/salsa_portal/>

## Juniper Netscreen- ISG 1000

*/!\Cannot access the GUI through CyberArk as it uses HTTPS. The GUI only supports HTTP for this devices.*

Use CyberAk to ssh the FWs on PARGUI2.

### ADS-T VPN Concentrator

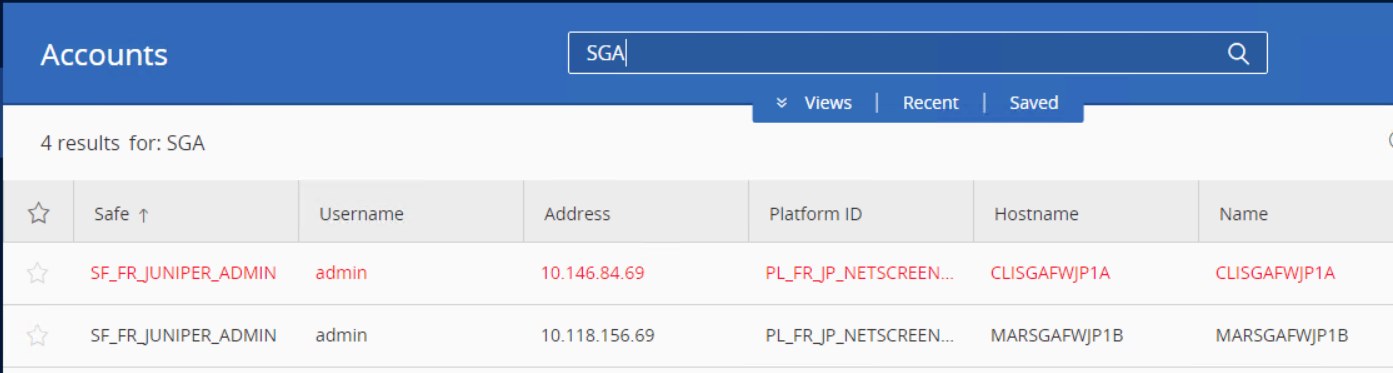


<http://clivpnn1.par.emea.cib/>

<http://marvpnn1.par.emea.cib/>

### SGA

*/!\ GUI access is not functional for these 2 GWs.*

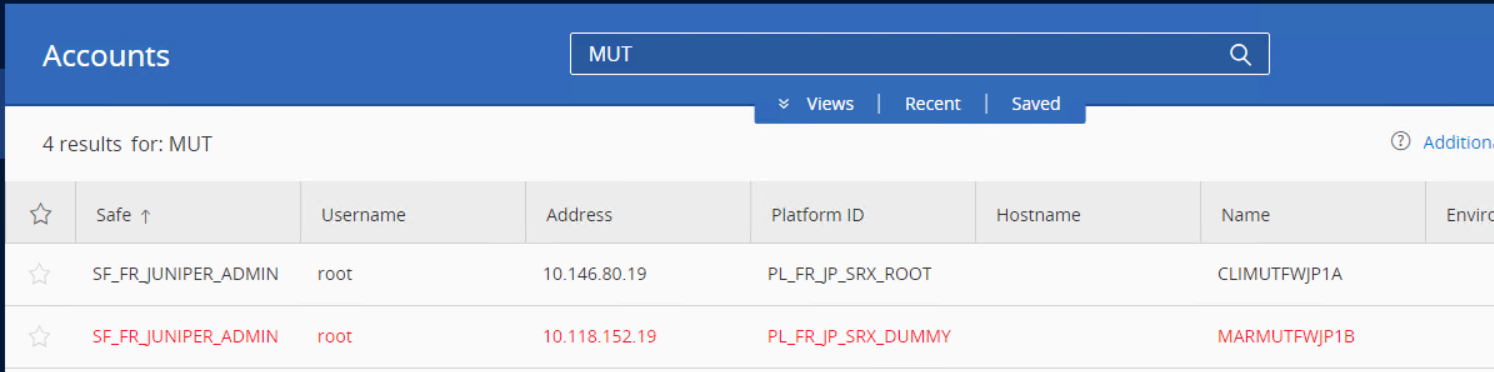


## Juniper SRX

Use CyberAk to ssh the FWs on PARGUI2.

*/!\Juniper NSM used to manage these gateways via a GUI is not functional.*

ADS-I



## Checkpoint ADS-I

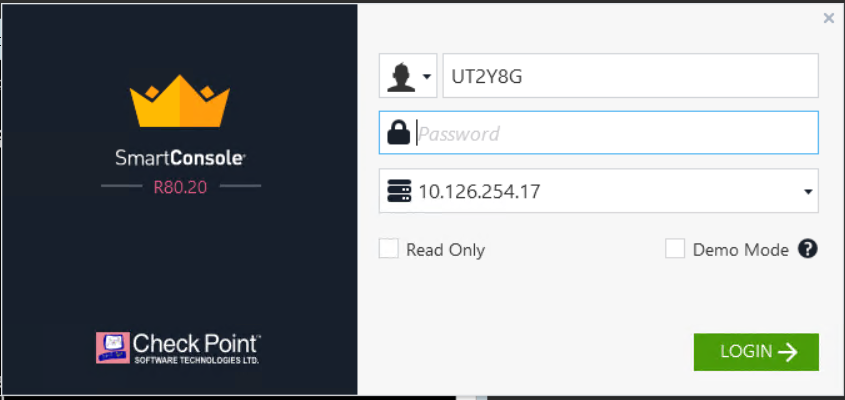
### MGMT console

*/!\ ask EMEA security admin to create a local UT account.*

Lauch SmartConsole R80.20 client on PARGUI1 10.126.254.14.

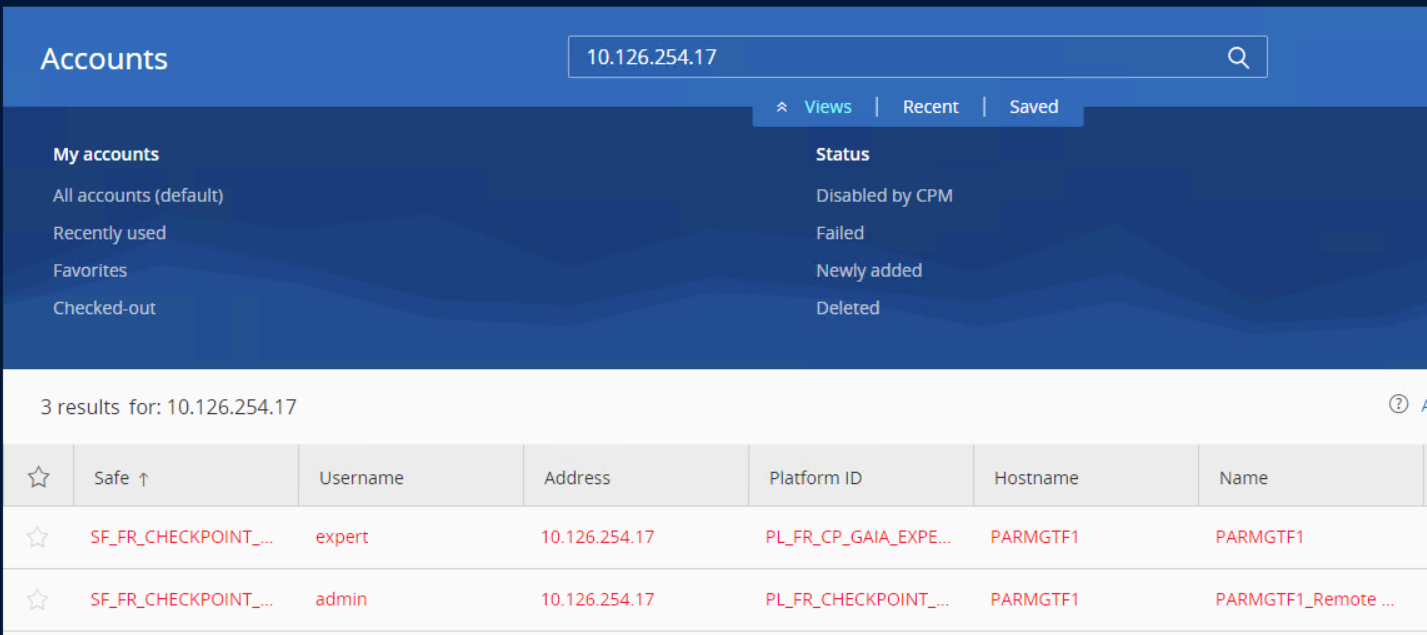
MDS IP @

parmgtf1.par.emea.cib: 10.126.254.17  
parmgtf2.par.emea.cib: 10.126.254.37



### Mutli-Domain Server and GWs

You can access Gaia portal and ssh (expert mode) checkpoint MDS and Gateways via CyberArk.



## Fortigate

*/!\ CyberArk access to the Fortigate GWs (GUI or SSH) is not functional.*

### FortiManager

*/!\ ask EMEA security admin to create a local UT account. Can also be accessed via CyberArk.*

https://10.126.254.56/

### FortiAnalyser

*/!\ ask EMEA security admin to create a local UT account.*

https://10.126.254.58/

## BIG IP F5

Use FireFox on PARGUI2 10.126.254.34.

*/!\ ask EMEA security admin to create a local UT accounts.*

Internet

Prod CLILBINTERF1-adm: <https://10.146.87.34/tmui/login.jsp>  
Prod MARLBINTERF1-adm: <https://10.146.87.35/tmui/login.jsp>

Qualif: <https://clilbinterf2.adm.cm.par.emea.cib/tmui/login.jsp>

Intranet

Prod clilbintf51a.par.emea.cib: <https://10.146.87.42/tmui/login.jsp>  
Prod marlbintf51a.par.emea.cib: <https://10.146.87.43/tmui/login.jsp>

Qualif: <https://clilbintraf2.adm.cm.par.emea.cib/tmui/login.jsp>

<https://10.146.86.46/tmui/login.jsp?msgcode=2&>  
<https://10.146.86.47/tmui/login.jsp?msgcode=2&>

ZI

clilbintf1b-adm.par.emea.cib:<https://10.146.86.46/tmui/login.jsp?msgcode=2&>  
marlbintf1b-adm.par.emea.cib: <https://10.146.86.47/tmui/login.jsp?msgcode=2&>

## Proxy McAfee

*/!\ ask EMEA security admin to create a Role mapping for your UTXXXX\_A account on the proxies.*

Internet

Use FireFox on PARGUI2 10.126.254.34. Choose “Web Gateway UI as in-browser HTML”

<https://clipxinterwg3-adm.par.emea.cib:4712/Konfigurator/request>

clipxinterwg3-adm.par.emea.cib: 10.146.82.167

clipxinterwg4-adm.par.emea.cib: 10.146.82.168

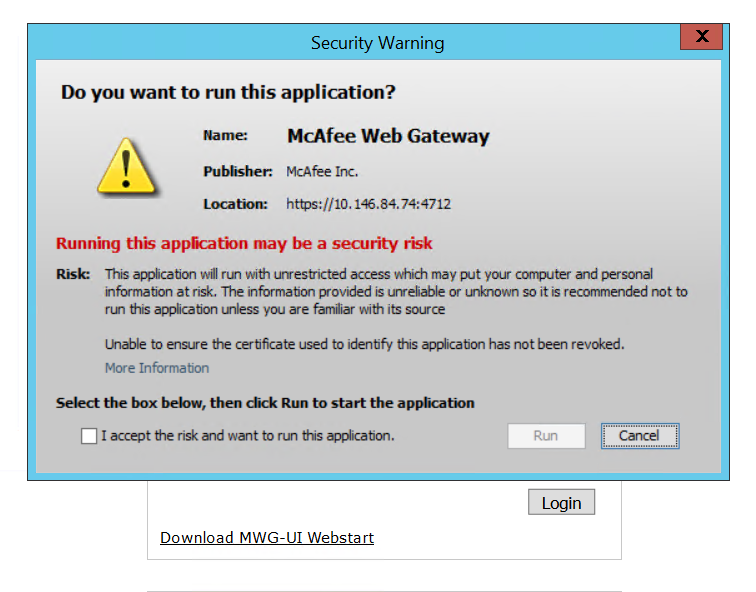
marpxinterwg3-adm.par.emea.cib: 10.118.154.171

marpxinterwg4-adm.par.emea.cib: 10.118.154.172

Intranet

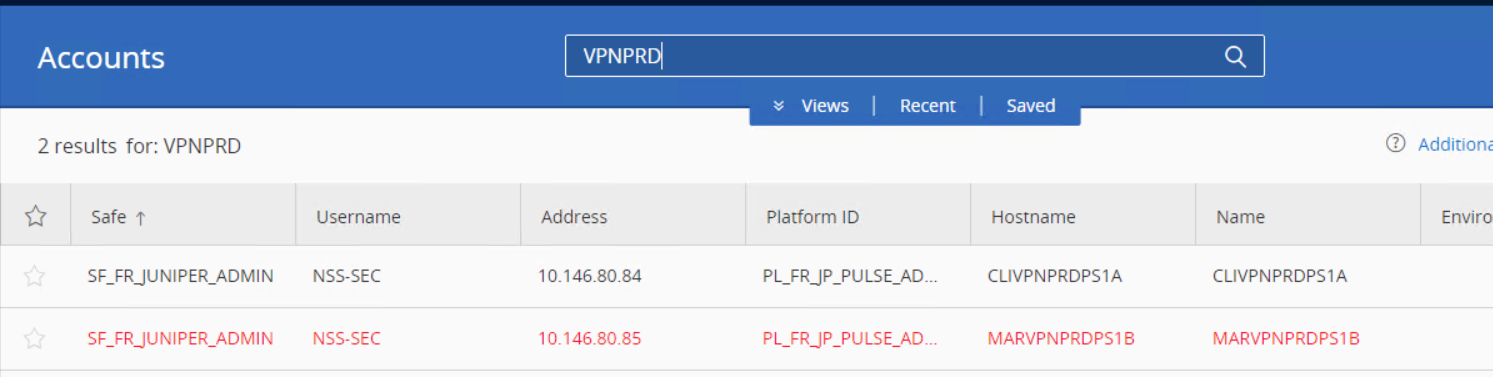
Use FireFox on PARGUI1 10.126.254.14. Choose “Download MWG-UI Webstart”  
  
<https://10.146.84.74:4712/Konfigurator/request>

clipxyintrawg1\_adm.par.emea.cib: 10.146.84.74  
marpxyintrawg1\_adm.par.emea.cib: 10.118.156.74



## Pulse Secure

Use CyberAk on PARGUI2 to access Pulse Secure GUI.



Prod  
clivpnprdps1a.par.emea.cib: <https://10.146.80.84/dana-na/auth/url_admin/welcome.cgi>  
marvpnprdps1b.par.emea.cib: <https://10.146.80.85/dana-na/auth/url_admin/welcome.cgi>

Qualif  
clivpnqualps1a.par.emea.cib: <https://10.146.80.23/dana-na/auth/url_admin/welcome.cgi>

## IPS TippingPoint

Lauch TippingPoint SMS client on PARGUI2 10.126.254.34. It is the same management console used for EMEA.

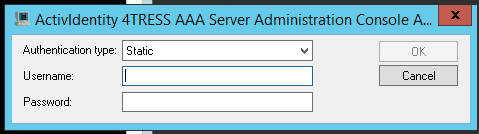
*/!\Ask security Admin for local* user account creation.



## Strong Authentication AAA

Launch ‘’Admin Console’’ client on PARGUI2 10.126.254.34.

*/!\Ask security Admin for local* user account creation.



# ASIA Infrastructure – network & security devices access

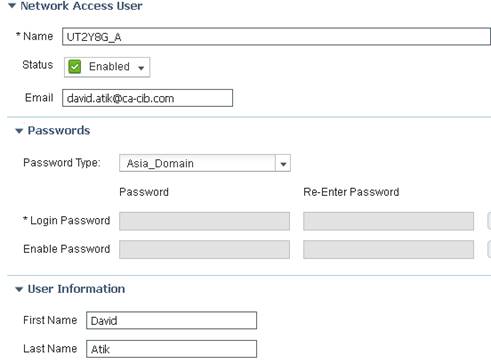


## GRANT Requests

|  |  |  |
| --- | --- | --- |
| **Application code** | **Application Name** | **Validation Path / Profile** |
| 1PADASIA | Privileged Active Directory Accounts - ASIA domain | ASIA.CIB AD account for ISAP-ITS users./ Administrator |
| 1FIRISAP | Infrastructure - Firewall Singapore | SuperAdmin  - Firewall – Singapore – ADM / SuperAdmin\_FIREWALL\_SGP\_SAFE\_admin |
| 1NDISAP | ISAP Network Devices | ISAP Network Devices / Administrator |
| 1CITISAP | Infrastructure - Checkpoint ISAP | SuperAdmin Checkpoint-DMZ ISAP / SuperAdm SAFE ADM |
| 1F5ISAP | Infrastructure - F5 ISAP | SuperAdmin Fortigate DMZ ISAP / SuperAdm SAFE ADM |
| 1FGEISAP | Infrastructure - Fortigate ISAP | SuperAdmin – Fortigate DMZ ISAP / SuperAdm SAFE ADM |
| 1JUISAP | Infrastructure - Juniper ISAP | SuperAdmin – Juniper DMZ ISAP / SuperAdm SAFE ADM |
| 1MAFISAP | Infrastructure - Mc Afee ISAP | SuperAdmin – Mac Afee DMZ ISAP / SuperAdm SAFE ADM |
| 1PRISAP | Infrastructure - Proxy Singapore | SuperAdmin  - Proxy – Singapore – ADM / SuperAdmin\_PROXY\_SGP\_SAFE\_admin |
| 1RAISAP | Infrastructure - Remote Access Server Singapore | SuperAdmin  - Remote Access – Singapore – ADM / SuperAdmin\_RA\_SGP\_SAFE\_admin |

## Network devices

Once your ASIA UTXXXX\_A is created, make sure your user access to ISAP/ASIA devices are granted on TACACS Cisco ISE by network Admin.



Connect to PARGUI2 (10.126.254.34) and then try to ssh eq02ilo2.isap.asia.cib - 10.129.1.202.

## Fortinet Ascenlink

Use Chrome on PARGUI2 10.126.254.34.

*/!\Ask ASIA Network Admin for local* user account creation.

ascenlink1.isap.asia.cib: <https://10.129.8.47>

ascenlink2.isap.asia.cib: <https://10.129.5.88>

## Cisco ISE

Use Chrome on PARGUI2 10.126.254.34.

*/!\Ask ASIA Network Admin for local* user account creation.

EQX eqwfise01 (Primary PAN & MnT): <https://10.129.4.144/admin/login.jsp>  
EQX eqwfise02 (Secondary PAN & MnT): <https://10.129.4.145/admin/login.jsp>  
NCS ncwfise01 (Secondary PAN & MnT):: <https://10.129.4.154/admin/login.jsp>  
NSC ncwfise02 (PSN Corporate): <https://10.129.4.155/admin/login.jsp>  
EQ eqwfdmzise1 (PSN Guest): 192.168.207.12  
NCS ncwfdmzise1 (PSN Guest): 192.168.207.142

## Cisco WLC

Use Firefox on PARGUI2 10.126.254.34.

*/!\Ask ASIA Network Admin for local* user account creation.

EQX eqwfwlc1 (Corporate) : <https://10.129.4.146/>  
NCS ncwfwlc1 (Corporate): <https://10.129.4.156/>

## Fortinet

Use Firefox on PARGUI2 10.126.254.34

|  |  |  |
| --- | --- | --- |
| ADS-L | SGPNCS01FG05 | [https://192.168.31.82](https://192.168.31.82/) |
| ADS-L | SGPNCS01FG06 | [https://192.168.31.83](https://192.168.31.83/) |
| Optim DR Firewall | SGPNCS01FG03 | https://192.168.31.75 |
| Optim DR Firewall | SGPNCS01FG04 | https://192.168.31.76 |
| DMZ (ADS-I Backend) | SGPEQX02FG01 | https://10.129.0.88 |
| DMZ (ADS-I Backend) | SGPEQX02FG02 | https://10.129.0.89 |
| DMZ (ADS-I Backend) | SGPNCS01FG01 | https://10.129.0.188 |
| DMZ (ADS-I Backend) | SGPNCS01FG02 | https://10.129.0.189 |
| Analazer | SGPNCS01FA01 | https://10.129.0.191 |
| Management | SGPEQX02FM01 | https://10.129.0.90 |
| Management | SGPNCS01FM02 | https://10.129.0.190 |
| DMZ Admin Firewall | EQ02TRMGTFW1-A | https://10.129.0.201 |
| DMZ Admin Firewall | EQ02TRMGTFW1-B | https://10.129.0.202 |
| DMZ Admin Firewall | NC01TRMGTFW-A | https://10.129.0.203 |
| DMZ Admin Firewall | NC01TRMGTFW-B | https://10.129.0.204 |
| VPN Firewall (RIA) | SGPEQX02FGRIA | https://192.168.82.84 |
| VPN Firewall (RIA) | SGPNC01FGRIA | https://192.168.31.85 |
| ADSL Firewall | SGPEQX02FG05 | https://192.168.82.85 |
| ADSL Firewall | SGPEQX02FG06 | https://192.168.82.86 |
| DMZ WIFI Firewall | NCWFDMZFW1 | https://192.168.201.6 |
| DMZ WIFI Firewall | EQWFDMZFW1 | https://192.168.45.6 |
| PBI extended VLAN Firewall | SGPNC01PBIFG01 | https://192.168.31.86 |
| PBI extended VLAN Firewall | SGPNC01PBIFG02 | https://192.168.31.86 |
| PBI extended VLAN Firewall | SGPEQ02PBIFG01 | https://192.168.82.90 |
| PBI extended VLAN Firewall | SGPEQ02PBIFG02 | https://192.168.82.90 |
| LPM SGP admin extended vlan | SGPNC01LPMFG01 | https://192.168.31.91 |
| LPM SGP admin extended vlan | SGPEQ02LPMFG01 | https://192.168.82.91 |
| AZQORE Firewall @ NCS | SGPNC01AZQFG1 | https://192.168.31.96 |
| AZQORE Firewall @ NCS | SGPNC01AZQFG2 | https://192.168.31.96 |
| AZQORE Firewall @ EQX | SGPEQ02AZQFG1 | https://192.168.82.94 |
| AZQORE Firewall @ EQX | SGPEQ02AZQFG2 | https://192.168.82.94 |
|  |  |  |

## Checkpoint

### Gateways

Use Internet Explorer on PARGUI1 10.126.254.14.

*/!\ username is case sensitive*

EQX Primary FW:              <https://192.168.82.77:4434/>

EQX Secondary FW:         <https://192.168.82.78:4434/>

NCS Primary FW:              <https://192.168.31.78:4434/>

NCS Secondary FW:         <https://192.168.31.79:4434/>

CHINA Checkpoint: <https://10.129.57.106/>

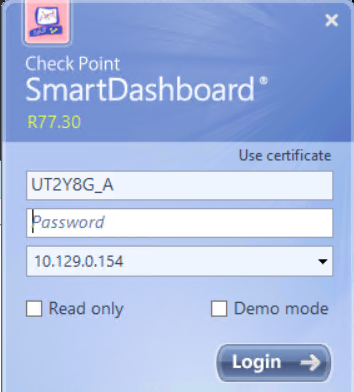
### Management Console

Lauch SmartDashboard R77.30 client on PARGUI2 10.126.254.34.

*/!\ username is case sensitive*

Checkpoint Management Smart-1 NCS: [10.129.0.154](https://10.129.0.154:4434/)

Checkpoint Management Smart-1 EQX: 10.129.0.54



## Juniper SSG

Use Firefox on PARGUI2 10.126.254.34

|  |  |  |
| --- | --- | --- |
| ADS-T - TKY | CT10TRW101 | [http://192.168.82.70](http://192.168.82.70/) |
| RIA VPN | SGPNC01TRRIA | http://192.168.31.70 |
| ADS-L | SGCT10TRF101 | http://192.168.82.72 |
| ADS-L | SGCT10TRF102 | http://192.168.82.73 |
| Etrali Firewall | SGPEQXETRAFW1 | http://192.168.82.74 |

## BIG IP F5

### Internal & DR

Use Chrome on PARGUI2 10.126.254.34.

|  |  |  |
| --- | --- | --- |
| Internal F5 | sgpeqx02f5prxy11 | [https://10.129.0.83](https://10.129.0.83/) |
| Internal F5 | sgpncs01f5prxy12 | https://10.129.0.183 |
| DR F5 | SGPCT10F5PRXY03 | https://10.129.0.84 |

### DMZ

*/!\For the DMZ F5, the authentication is Local only as this cannot be integrated with CyberArk.*

*Ask ASIA security Admin for local* user account creation.

*/!\ username is case sensitive*

|  |  |  |
| --- | --- | --- |
| DMZ F5 | SGPEQ02F5PRXY03 | https://192.168.82.82 |
| DMZ F5 | SGPEQ02F5PRXY04 | https://192.168.82.83 |
| DMZ F5 | SGNCS01F5PRXY03 | https://192.168.31.80 |
| DMZ F5 | SGNCS01F5PRXY04 | https://192.168.31.81 |

## Pulse Secure

Use FireFox on PARGUI2 10.126.254.34.

EQX  - <https://192.168.82.95/dana-na/auth/url_admin/welcome.cgi>

NCS - <https://192.168.31.97/dana-na/auth/url_admin/welcome.cgi>

## Proxy McAfee

Use FireFox on PARGUI2 10.126.254.34. Chose “Web Gateway UI as in-browser HTML”

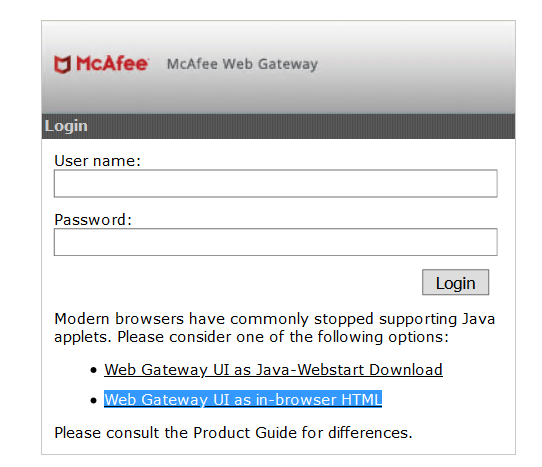
NCS Proxy : <https://192.168.31.73:10000/Konfigurator/request>

EQX Proxy: <https://192.168.82.80:10000/Konfigurator/request>

CHINA Proxy: <https://10.129.57.109:10000/Konfigurator/request>

WIFI Proxy NCS: <https://192.168.201.13:10000/Konfigurator/request>

WIFI Proxy EQX: <https://192.168.45.12:10000/Konfigurator/request>



## IPS TippingPoint

Lauch TippingPoint SMS client on PARGUI2 10.126.254.34. It is the same management console used for EMEA.

*/!\Ask Admin for local* user account creation.



## AAA Active Identity

Use FireFox on PARGUI2 10.126.254.34.

*/!\Ask ASIA security admin for the admin account*

<http://10.129.5.139:8080/pack/helpdesk/login>

<http://10.129.5.78:8080/pack/helpdesk/login>

## MRTG/CACTI

Accessible from LAN using normal UTXXXX code.  
<http://asiamrtg.isap.asia.cib/index.php>

## PAC file Folder

Accessible from LAN using.  
[\\10.129.12.105\Proxypac](file:///\\10.129.12.105\Proxypac)

## Asia Active Directory

Run as administrator on your local computer ‘’dsa.msc’’ and make sure you have RW access.

*/!\Ask ASIA security admin to give you RW access.*

