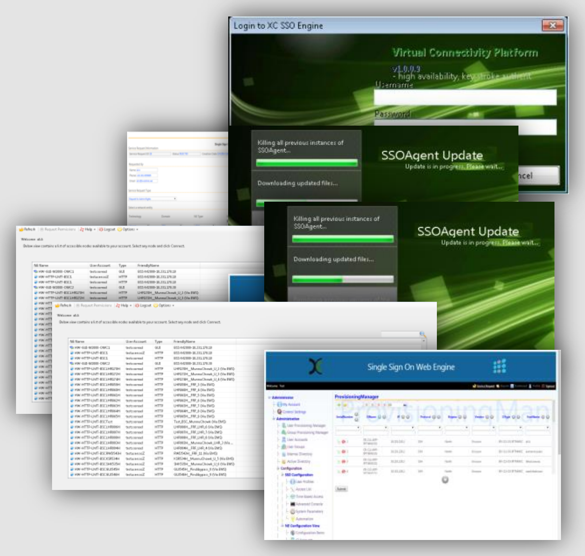
exceleron
communications

Single Sign-On System

COMPLETE SYSTEM ADMIN AND SECURITY SUITE

Exceleron Communication Solution Guide



Login to XC SSO Engine
Virtual Connectivity Platform
Username
Password
Killing all previous instances of SSOAgent...
Downloading updated files...
SSOAgent Update
Update is in progress. Please wait...
Single Sign On Web Engine
ProvisioningManager

Exceleron Communications (Pvt.) Ltd.

INTRODUCTION

Single sign on solution is specifically used by engineers to interact with network applications and devices in a centralized and secured environment. It is targeted to overcome challenges in the telecommunication/IT network where staff interacts directly with NE/Application servers with less security and without any centralized administrative control. Single sign on system help to implement consistent set of security procedures and policies throughout the entire network.

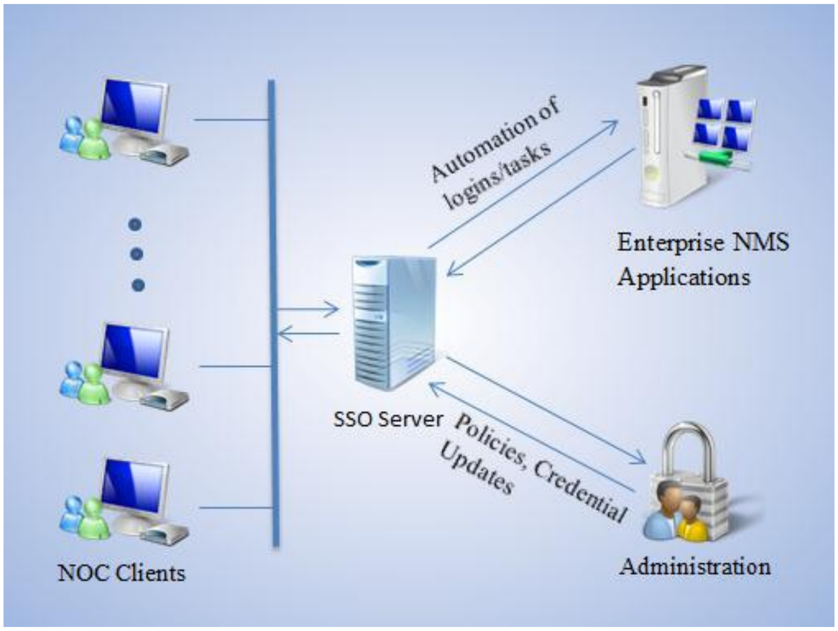
BENEFITS DELIVERED

- Ability to have one user login across all applications.
- Distinct user identification with flexible authentication mechanisms (including standard username/password, System generated keys and Radio frequency identification tags)
- Centralized management of identities for all applications.
- Reduced administrative overheads – process improvements and reduction in cost.
- Improved platform security for network elements.
- Easy to utilize user interface through Single Sign-on for navigating between applications.
- User productivity improvements with Single Sign-on for all the applications.
- Ease of integrating new systems in the future without security administration constraints.
- Fine grained control by specifying securing policies with precise set of commands and filtering rules for each NE CLI session.
- Supporting integration with corporate systems. (employee’s active directory)
- Improving system administrators control and better visibility of user activities.
- Customizable reporting to SSO administrator for each user session.
- Improving time and cost for network operator in terms of re-work, staffing, network fail-over

FUNCTIONAL DESCRIPTION

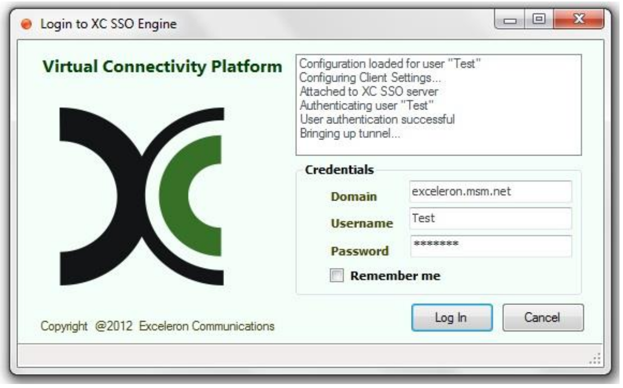
Users can logon to SSO server portal (with Username/Password or using automatic Radio frequency identification tags) and gains access to multiple applications within an enterprise based on their profiles without being prompted to log in again at each of them.

SSO server is utilized for one-time user authentication to access network elements/ applications. It can internally translate different credentials for NE/Applications with user account and provide virtual access to the required NE. SSO administrator can configure user profiles, specific roles/privileges, NE/Application credentials etc. in SSO server.


Automation of logins/tasks
Enterprise NMS Applications
SSO Server
Policies, Credential Updates
Administration
NOC Clients

SINGLE SIGN-ON SECURITY POLICY MANAGER (SPM)

Security policy manager is the core of SSO system. There is a single interface for the users to interact all NEs and EMS in the network. A unique user identity is authenticated through its internal Active directory DB or through any external Employee active directory. Three-way authentication can be implemented where users can be authenticated by proximity devices at first phase, a unique username and password is then generated in the second phase and send to user by SMS. In the third phase, user can then login to SSO portal with Active Directory credentials.



Login to XC SSO Engine

Virtual Connectivity Platform

```
Configuration loaded for user "Test"
Configuring Client Settings...
Attached to XC SSO server
Authenticating user "Test"
User authentication successful
Bringing up tunnel...
```

Credentials

Domain: exceleron.msm.net

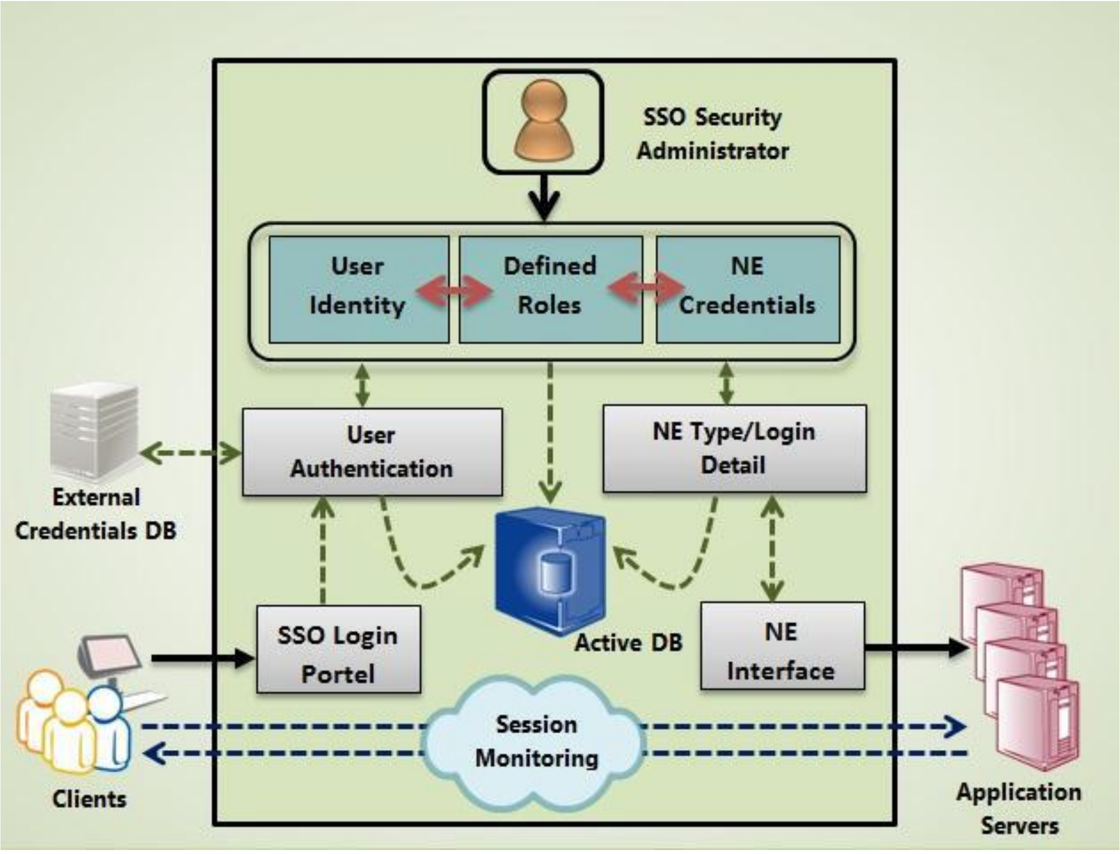
Username: Test

Password: *******

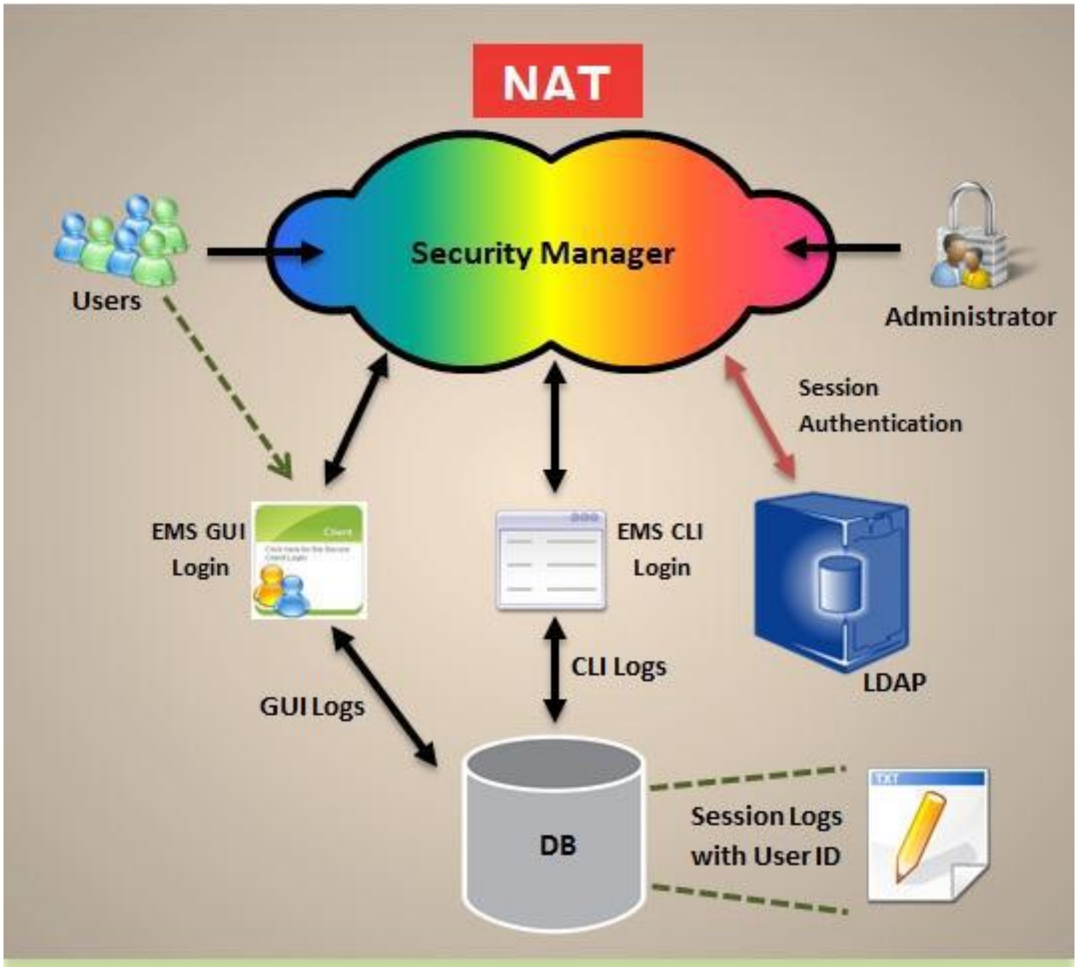
□ Remember me

Copyright @2012 Exceleron Communications

The administrator can define specific roles to a user that determine the applications, commands, and NEs that can be accessed by the user based on job profile. Administrator can also implement security policies by providing network-wide security management of users, NEs and EMSs via a single tool. Virtual user session is available to users using Security Proxy Server instead of logging directly onto any given NE or EMS.



SPM launches access to the selected terminal of NE or system on user request. For accessing the servers via GUI, a light sign-on utility runs on the front end user machines to support GUI session. Command-line sessions like SSH, Telnet and FTP appear as if the user is directly logged into the device but the user's access privileges and sessions is under supervision of security policy manager. All command-line and GUI interaction is logged in the SSO DB store for security purposes.



SINGLE SIGN-ON USER AUTHENTICATION

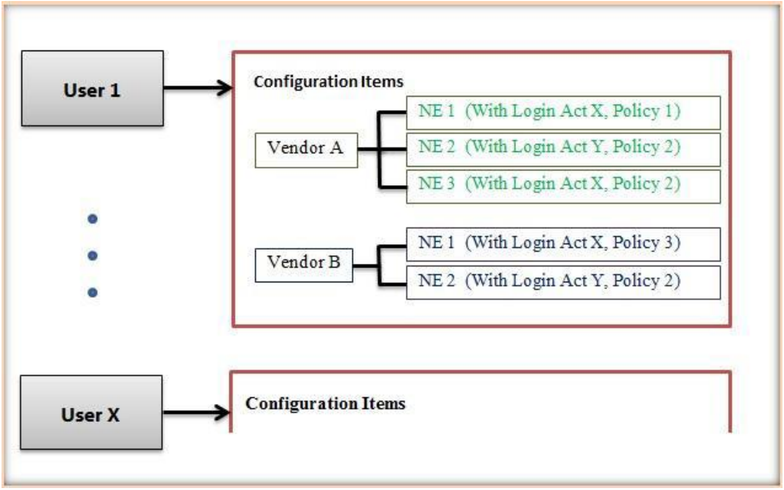
SSO system improves security through the reduced need for a user to handle and remember multiple sets of authentication information. Unique user Identity is required to login to SSO proxy server, SSO Security manager internally performs automated username and password mapping of OMC/EMS/IT devices privileged accounts.

User credentials for SSO proxy server can be authenticated via

- LDAP (Employee Directory Systems)
- XC SSO Internal database
- External Corporate Systems database (Oracle, SQL Server, DB2, Sybase)
- Combination of any of the above

SINGLE SIGN-ON USER PRIVILEGES

User sessions with Network Elements can be assigned very specific privileges to eliminate the risk of granting greater access to users by security administrator. Highly tailored NE authorization privileges, can be created, irrespective of how many NE accounts exist. Security administrators can customize each user’s access privileges by specifying securing policies with precise set of commands he or she is authorized to use. Security policies can define filtering rules for each NE (such as switches, routers, or application servers). Filtering rules also supports various IP layer protocols (like SSH, Telnet, FTP, etc.) or telecom-specific protocols.


User 1
Configuration Items
Vendor A
NE 1 (With Login Act X, Policy 1)
NE 2 (With Login Act Y, Policy 2)
NE 3 (With Login Act X, Policy 2)
Vendor B
NE 1 (With Login Act X, Policy 3)
NE 2 (With Login Act Y, Policy 2)
User X
Configuration Items

SINGLE SIGN-ON SYSTEM CONFIGURATION

Following system Configurations can be done by SSO Administrator in ready to use SSO version.

Element	Detail
Configuration Item	All NE Devices are defined in the system. (Source IP, port, supported authentication protocols, Session protocols etc.)
Accounts Inventory	All NE accounts detail with credentials are stored in the system
Securing Access policy	Access policies are defined by applying commands/protocols filtering rules to any NE or group of NEs. Session Monitoring rules are also defined.
User Account	Users are defined with their respective roles/privileges (Accounts Detail). Assign any combination of NE or group of NEs with securing policies.
User Inventory	User Authentication modes are defined

REAL TIME LOGGING

There are three types of Logging features available in the system

Command Logging:

Each command that is run from the XC terminal window from any client can be logged inside the internal XC database. By default, all commands are tagged to get logged. However, the administrator has the rights to run on/off logging on any client or user. There is also an option to log the output of the commands as well. From the front web view, administrators or privileged users can create a complete log of the activity at any terminal during any time-interval he selects.

Video Logging:

All the GUI sessions are recorded in lossless differential PNG compressed frames and stored on the disk. There are various options of recording including, High Definition, 256-color, grey-scale, etc. This defines the quality and size of the logged video. From the front web view, administrators or privileged users can create a complete video of the activity at any terminal during any time-interval he selects.

Internal Logging:

The system logs all the actions performed by users in its internal database and these are visible over the web frontend to the administrators. System also logs all the actions it performs itself. In addition, all the erroneous conditions can be forwarded as traps via SNMP to the NMS via NBI-module.