Avaya
Communication Server 1000
Security Domain Guide

Issue 1.12.2
13 March 2012

ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE INFORMATION PROVIDED HEREIN WILL ELIMINATE SECURITY THREATS TO CUSTOMERS’ SYSTEMS. AVAYA INC., ITS RELATED COMPANIES, DIRECTORS, EMPLOYEES, REPRESENTATIVES, SUPPLIERS OR AGENTS MAY NOT, UNDER ANY CIRCUMSTANCES BE HELD LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE INFORMATION PROVIDED HEREIN. THIS INCLUDES, BUT IS NOT LIMITED TO, THE LOSS OF DATA OR LOSS OF PROFIT, EVEN IF AVAYA WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF THESE TERMS.

Table of Contents

Avaya Communication Server 1000 Security Domain Guide

Version History

Issue	Change Summary	Author(s)	Date (yyyy-mm-dd)
1.01	Initial version.	Alain Coutu, Ping Lin	2011-04-20
1.02	Updated the Primary and Backup Security Server Installation and Creating a Security Domain sections.	Alain Coutu, Ping Lin	2011-04-20
1.03	Applicable Documentation section added. Updated Applicable Releases, ELAN/TLAN Usage, Registering Elements to the Security Domain, Registering VxWorks-Based Servers and Devices, Registering Linux-Based Servers, Security Domain Users and Patches sections.	Alain Coutu, Ping Lin	2011-04-25
1.04	Updated version history, ELAN/TLAN Usage, Primary and Backup Security Server Installation, Security Domain Users and Patches sections. Added Table of Contents, Troubleshooting and Security Domain Checklist sections.	Alain Coutu, Ping Lin	2011-04-27
1.05	Updated based on comments from review with AT&T.	Alain Coutu, Ping Lin	2011-04-29
1.06	Updated based on comments from AT&T.	Alain Coutu, Ping Lin	2011-05-05
1.07	Updated based on comments from AT&T and TSSR group.	Alain Coutu, Ping Lin	2011-05-12
1.08	Updated ELAN/TLAN Usage section to address the case of non-routable or non-extended ELAN subnets.	Alain Coutu, Ping Lin	2011-05-25
1.09	Added security domain FAQ.	Greg Brazil	2011-06-09
1.10	Synced up LAN configurations with NTP and added appendix on configuring static routes.	Greg Brazil, Alain Coutu, Ping Lin	2011-06-24
1.11	Added some clarification on registration of VxWorks vs. Linux elements.	Alain Coutu, Ping Lin	2011-07-29
1.12.1	Updated privileges for LD 117 commands in appendix.	Alain Coutu, Ping Lin	2011-08-23
1.12.2	Updated ELAN/TLAN Usage section to address the case of UCM deployed on SMGR.	Henry Yang, Ping Lin	2012-03-13

Applicable Releases

The content of this document is applicable to the Avaya Communication Server 1000 Release 6.0 and higher.

Applicable Documentation

The information contained in this document is in addition to the information currently documented in the following Avaya CS 1000 documents:

- NN43001-116: Unified Communications Management Common Services Fundamentals
- NN43001-260: Converging the Data Network with VoIP Fundamentals
- NN43001-315: Linux Platform Base and Applications Installation and Commissioning
- NN43001-604: Security Management Fundamentals
- Avaya Communication Server 1000 Port Matrix Document for Releases 6.0, 7.0 and 7.5
- Enterprise Voice Solutions Patch Reference and Best Practice Guidelines, v1.3
- CS 1000 Release 6.0 Systems: Service Pack Installation Requirements, dated 5 Apr 2011 (check for latest update)
- CS 1000 Release 7.0 Systems: Service Pack Installation Update, dated 22 Mar 2011 (check for latest update)
- CS 1000 Release 7.5 Dependency List and Service Pack Now Available, dated 18 Jan 2011 (check for latest update)

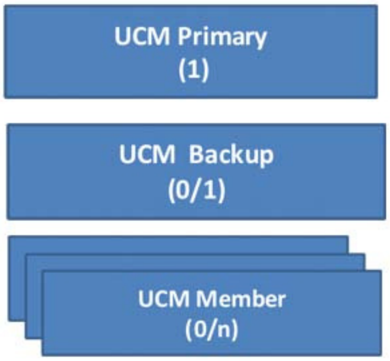
Overview of UCM Security Domain

The UCM security domain provides central authentication, authorization, auditing, certificate management, and secure navigation functionality between managed elements. All elements within the same security domain appear in a single navigation tree. UCM Common Services provides features and capabilities for all installed elements. When a user logs on to UCM Common Services, it is not necessary to re-authenticate to access a different element within the security domain. This is what is known as the Single Sign-On capability.

Registering with the UCM security domain establishes mutual trust between the UCM primary security server and all other elements in the security domain. This enables system operations and communications to function normally. Elements that are not members of the security domain are non-trusted and will experience limitations in features that require secure communications to trusted elements, such as file transfer. Therefore, to ensure proper system operability and security, all elements in a system must be members of the same UCM security domain.

A UCM security domain is defined by the UCM primary security server, and comprises the UCM primary security server, the UCM backup security server, and associated member servers.

The primary security server must be the first server deployed in the security domain. The security domain can have 0 or 1 backup servers and additional servers are member servers, as shown in the following figure.



Security Domain

Only one primary security server is required on a network. This server stores and provides write access to all administrator identities, authorization data, and security configuration data. It handles all authentication, authorization and audit log consolidation requests, and also provides a private certificate authority to issue certificates to member servers. Administrators use the primary security server for navigation to UCM Common Services, network navigation, and as the launch pad for network applications such as Subscriber Manager. Note that configuration of all options in UCM Common Services, as well as access to the certificate management pages, are only available from the primary security server.

The role of the backup security server is to manage authentication, authorization and audit log consolidation requests when the primary server cannot be contacted. The backup security server is optional, and there can be at most one backup security server on a network. Also, since the backup security server is read-only, you cannot use it to configure changes such as adding new administrators.

Other than the primary and backup security servers, all other servers in the security domain are member servers, whose security requests are served by the primary and/or backup security servers. For emergency situations when neither the primary nor backup security server can be contacted, you can use the local logon page on the member server.

ELAN/TLAN Usage

The LAN configuration for the CS 1000 is described in *Converging the Data Network with VoIP Fundamentals, NN43001-260*.

When designing a network for the CS 1000, there are four different configurations that can be implemented. They are:

1. Normal configuration: This configuration is also referred to as the “Routed configuration”. It is intended to serve most customers with larger systems, multiple call servers, or requiring SNMP access. In addition if a customer plans to implement multiple ELAN subnets or multiple CS 1000 systems within the same UCM security domain, this configuration is preferred.
2. Small configuration: This configuration is best suited for single system installations with no SNMP access and a single ELAN subnet interconnecting all of the CS 1000 dependent elements.
3. Managed Services configuration: This configuration is intended to serve the management of multiple networks or multiple call servers where complete isolation between the ELAN or “Signaling and Management Network” and the various “Enterprise Networks” is required.
4. Hybrid Managed Services configuration: This is a hybrid of the Normal and Managed Services configurations.

Independent of the LAN configuration implemented at a customer site, the following points apply:

- The PC used for web browser access to UCM should be connected to the TLAN (except in the case of the Managed Services configuration). If no DNS server is in use the PC hosts file should include an entry containing the TLAN IP address and FQDN of the primary security server. Note that editing the hosts file on Windows generally requires administrator access.

- When registering VxWorks elements (such as MGCs, MGSs, VGMCs, MC32s, MC32Ss, and Call Servers which are not on co-resident Call Server / Signaling Server systems), use the ELAN IP address of the UCM primary security server.
- When registering Linux elements (such as Signaling Servers, and co-resident Call Server / Signaling Server systems and the Call Servers on these systems), use the TLAN FQDN or IP address of the UCM primary security server.

- The UCM security server must be capable of communicating to all elements that it is managing independent of the location of the elements on the network (ELAN or TLAN). Static routes may be necessary. Refer to the section titled “Configuration of Static IP Routes” in *Converging the Data Network with VoIP Fundamentals, NN43001-260*.
- In particular, for CS 1000 Release 7.5 or higher, if SMGR is deployed (SMGR 6.1 and above include the functionality of UCM) in the network, since SMGR uses a single IP address which is usually on the TLAN, configuration is required to ensure communication between SMGR and elements such as Call Servers that are located on the ELAN.

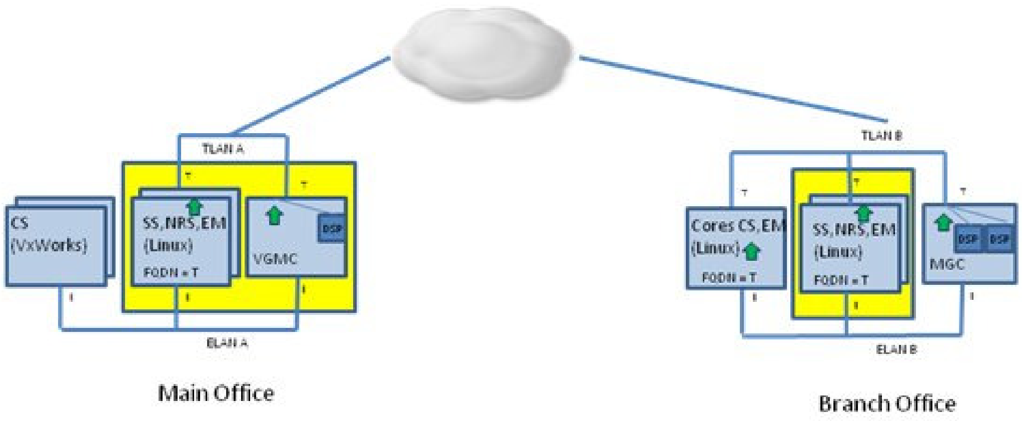
- If a network has multiple ELAN subnets, static routes must be created to ensure communication between the UCM security server and the elements residing on the ELAN subnets.

- Manual routes are required to all remote Intra-System Signaling and Management Network (ISSMN) subnets via the ELAN gateway on all elements.

- SNMP access requires ELAN connectivity to the UCM security server.
- Web management traffic is executed using the TLAN interface.
- CLI access to VxWorks elements can be accomplished using the Virtual Terminal application in CS 1000 Element Manager. Note that Virtual Terminal runs over the ELAN interface, and the PC will need to be able to route to the ELAN. This cannot be done if the ELAN is on an isolated network from the TLAN. (Virtual Terminal is not proxied by the Element Manager except for the CLI CSLOGIN command. The Signaling Server will proxy the RLOGIN session.)

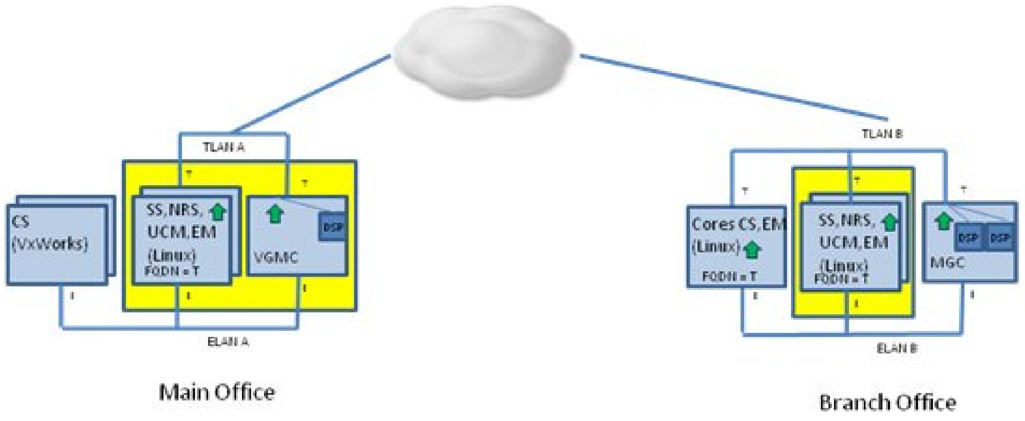
- Firewalls can be installed between elements. The most accurate port specifications for each of the CS 1000 releases governed by this document can be found in the associated Port Matrix Documents at the following link: http://support.avaya.com/css/appmanager/public/support?_nfpb=true&_pageLabel=WNContent_Public&contentid=C201082074362003

Note that due to the requirement to ensure communication between the UCM security server and elements located on multiple ELAN subnets described above, configurations involving non-routable or non-extended ELAN subnets will require the configuration of separate security servers for each ELAN subnet. An example of this is the pre-Release-6.0 customer network configuration where main and branch office ELANs are segregated from each other as shown in the following figure.



- The main and branch offices are segregated from each other
- TLANs are made routable and can be accessed from both locations
- ELANs are not made routable and are not extended thus are local to each location

When upgrading to Release 6.0 or higher, if it is still desired that the ELANs remain segregated (non-routable / non-extended), separate UCM primary security servers will need to be configured for each location.



- The main and branch offices are segregated from each other
- TLANs are made routable and can be accessed from both locations
- ELANs are not made routable and are not extended thus are local to each location
- UCM primary security servers at each location because of ELANs not being routable or extended

Primary and Backup Security Server Installation

It is good practice to perform regular system backups. Doing so will protect configuration information and significantly decrease the time required for restoration of the system during a software upgrade, system installation or an outage. The single largest delay factor in system recovery is related to a lack of current system backups. Before performing any significant activities related to the security server, system and application backups are strongly recommended. Information on performing backups is contained in the Linux Platform Base and Applications Installation and Commissioning, NN43001-315 document.

Installing and Configuring the Primary Security Server

The primary security server is a Linux-based server which is installed using the procedures described in Linux Platform Base and Applications Installation and Commissioning, NN43001-315.

The Fully Qualified Domain Name (FQDN) should be determined prior to installing the primary security server. Avaya strongly recommends that you do not change the FQDN and host name of the primary and backup security servers after security configuration has been completed due to the FQDN's integration with the private certificate authority of the security domain. In the event the FQDN must be changed after installation, refer to the procedures and warnings in Unified Communications Management Common Services Fundamentals, NN43001-116.

Note: The FQDN of the primary security server is associated with the TLAN IP address of the server. In other words, although the primary security server is also connected to the ELAN, it should always be configured using the TLAN.

Also, the primary security server must be fully patched prior to any other configuration activity or server installation, as it hosts the patch manager for all other servers and devices. See the "Patches" section for more information.

After the installation of Linux Base, the primary security server is configured as described by the following procedure:

Note: If using a DNS server, the DNS server must be configured before proceeding.

1. In the web browser address bar, type **https://<FQDN>** of the primary security server and press **Enter**.

2. On the Security Configuration page, select **Full security configuration**.
3. Click **Security Configuration**. The **FQDN validation** page appears.
4. Confirm that the (TLAN) IP address and FQDN are correct, and click **Next**. The **Select server type** page appears.
5. Select **Primary security server**, and click **Next**. The **Enter server information** page appears.
6. In the **Administrator password** field for the built-in "admin" account, type the new password. The password must contain a minimum of eight characters with:
    - At least one number from 0 to 9
    - One special character such as an underscore (_)
    - One upper- and one lower-case character

    Allowed characters in the password are: a-z A-Z 0-9 {}|()<>,/.=[]^~ _@!'$%&-+":?`\'
    The built-in "admin" account has the UCM Network Administrator role by default.
7. In the **Confirm Administrator password** field, re-type the new password.
8. Click **Next**. The **Enter certificate information** page appears.
9. Configure the following values:
    - Friendly name: A string to identify the certificate
    - Bit length: Number of bits (512, 1024 or 2048) in the key used for encryption
    - Organization: Your company name
    - Organizational unit: A division within your company
    - Common name: FQDN of the primary security server
    - Country/Region: The country where the primary security server is located
    - State/Province: The state/province where the primary security server is located
    - City/Locality: The city/locality where the primary security server is located
10. Click **Finish**. The **Security Configuration Progress** page appears.
11. Click **Restart** to restart the web server for the security configuration changes to take effect. The **Security Configuration Progress** page confirms that the server is restarting.

Note: Restarting the web server affects all applications, which are offline during the restart. Close the web browser window and wait for the server to reboot before attempting to log back on.

After the web server restarts, you can validate that the primary security server has been successfully installed and configured by logging on to **https://<PrimarySecurityServerFQDN>** with the "admin" account and the recently configured administrator password. The UCM Elements page should display.

Installing and Configuring the Backup Security Server

The backup security server, like the primary security server, is also a Linux-based server which is installed using the procedures described in *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Note: The FQDN of the backup security server is associated with the TLAN IP address of the server. In other words, although the backup security server is also connected to the ELAN, it should always be configured using the TLAN.

Note: If when installing and configuring the backup security server the ELAN IP address was used to join the security domain, the recommended course of action to correct this issue is:

1. Shut down the backup security server.
2. Remove the backup security server as an element from the primary security server.
3. Rebuild the backup security server.
4. Rejoin the security domain.

The backup security server should be fully patched before registering elements to the security domain. See the "Patches" section for more information.

The following procedure details the steps for configuring the backup security server at Linux Base installation time:

Note: If using a DNS server, the DNS server must be configured before proceeding.

Note: Ensure that the primary security server is configured and running before configuring the backup security server.

1. In the web browser address bar, type **https://<FQDN>** of the backup security server and press **Enter**.
2. On the Security Configuration page, select **Full security configuration**.
3. Click **Security Configuration**. The **FQDN validation** page appears.
4. Confirm that the (TLAN) IP address and FQDN are correct, and click **Next**. The **Select server type** page appears.
5. Select **Backup security server**, and click **Next**. The **Enter server information** page appears.
6. Enter the (TLAN) IP address of the primary security server and click **Next**. The **Verify primary security server fingerprint** page appears.
7. Verify the FQDN and fingerprint of the primary security server. If they are valid, type a primary security server user ID that has the UCM Network Administrator role and its password, and click **Next**. The **Enter certificate information** page appears.
8. Configure the following values:
    - Friendly name: A string to identify the certificate
    - Bit length: Number of bits (512, 1024 or 2048) in the key used for encryption
    - Organization: Your company name
    - Organizational unit: A division within your company
    - Common name: FQDN of the primary security server
    - Country/Region: The country where the backup security server is located
    - State/Province: The state/province where the backup security server is located
    - City/Locality: The city/locality where the backup security server is located
9. Click **Finish**. The **Security Configuration Progress** page appears.
10. Click **Restart** to restart the web server for the security configuration changes to take effect. The **Security Configuration Progress** page confirms that the server is restarting.

Note: Restarting the web server affects all applications, which are offline during the restart. Close the web browser window and wait for the server to reboot before attempting to log back on.

After the web server restarts, you can validate that the backup security server has been successfully installed and configured by logging on to **https://<BackupSecurityServerFQDN>** with the “admin” account and its password. The UCM Elements page should display.

Security Domain

Creating a Security Domain

There are no specific actions for creating a security domain. Once installation and configuration of the primary security server is complete and the server is up and running, the security domain is implicitly established.

Registering Elements to the Security Domain

Note: Ensure that the primary security server (and backup security server if one is used in the network) is/are configured and running before registering elements.

Registering VxWorks-Based Servers and Devices

Note: A CLI (telnet, rlogin or ssh) connection is needed to use security domain registration commands.

VxWorks-based servers and devices can register to the security domain in either of the following modes:

- User mode (**preferred**) — This mode is easiest to use and obviates the need to use a manual mode command on each individual server or device. The registration/un-registration operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed using the following command:
    - LD 117: **[Register / Unregister] UCMSecurity System**
- Manual mode — The registration/un-registration operation is performed on each individual Call Server, Gateway Controller and VGMC using the following commands:
    - LD 117: **[Register / Unregister] UCMSecurity [CS / Device]**
    - OAM/PDT CLI: **joinSecDomain** or **leaveSecDomain**

Before issuing the commands to register to the security domain, ensure that all elements are active and known to the Call Server. Also, when upgrading a pre-Release-6.0 CS 1000 to Release 6.0 or higher, ensure that secure transfer (sFTP) is turned off before transferring loadware and registering all MGCs, VGMCs and MCs to the Call Server. Turn sFTP on after successfully registering these devices to the Call Server and before registering them to the security domain.

Registration status can be viewed using the following commands:

- LD 117: **Stat UCMSecurity System**
- OAM/PDT CLI: **statSecDomain**

Note: On co-resident Call Server / Signaling Server systems, the **Register / Unregister UCMSecurity CS** commands are actually just used to turn central UCM authentication on/off for the Call Server, since the Call Server is automatically registered to the security domain as part of registering the overall system at Linux Base installation time.

Note: High Availability (HA) Call Servers must be in redundant mode to properly register to the security domain. If the Call Server is split for any reason, it must re-register to the security domain once a successful join command is issued.

Registration/un-registration operations work differently in redundant, split and single modes:

- Redundant mode: LD 117 registration/un-registration commands must be issued form the active core and are then mirrored between the active and inactive cores.
- Split mode: If LD 117 registration/un-registration commands are issued from the active core, they will apply only to the active corre and devices associated with it, and the inactive core will remain unregistered. Registration commands should not be issued from the inactive core except as part of a diagnostic process.
- Single mode: The un-registration commands may be used while in single mode if required. Registration commands should not be issued from an HA system when in single mode; While in single mode both cores will identify themselves as the active CPU when connected to the LAN. HA redundancy should be restored prior to attempting registration with the security domain.

Registering Linux-Based Servers

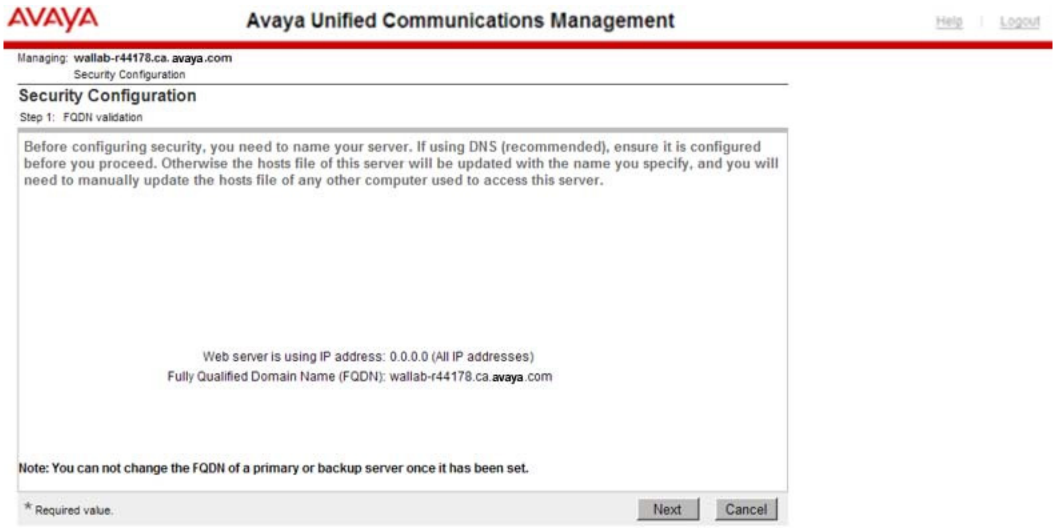
Linux-based servers register to the security domain at Linux Base installation time. Base Manager is used to perform registration. To access Base Manager, type **https://<FQDN>** of the server being registered in the web browser address bar and press **Enter**.

Note: If when installing and configuring a member server the ELAN IP address was used to join the security domain, the recommended course of action to correct this issue is:

1. Remove the member server as an element from the primary security server.
2. Rejoin the security domain.

The following procedure shows the registration steps in detail:

1. From the Security Configuration page, select the **Full security configuration** radio button and click **Security Configuration**. The **FQDN validation** page appears.



Managing: wallab-r44178.ca.avaya.com
Security Configuration

Security Configuration
Step 1: FQDN validation

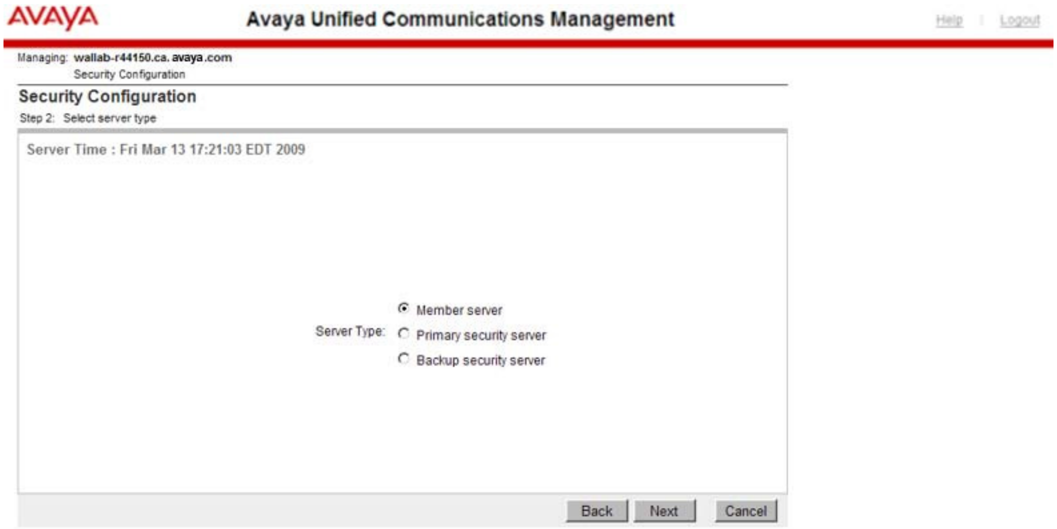
Before configuring security, you need to name your server. If using DNS (recommended), ensure it is configured before you proceed. Otherwise the hosts file of this server will be updated with the name you specify, and you will need to manually update the hosts file of any other computer used to access this server.

Web server is using IP address: 0.0.0.0 (All IP addresses)
Fully Qualified Domain Name (FQDN): wallab-r44178.ca.avaya.com

Note: You can not change the FQDN of a primary or backup server once it has been set.

* Required value.

2. Confirm that the (TLAN) IP address and FQDN are correct, and click **Next**. The **Select server type** page appears.



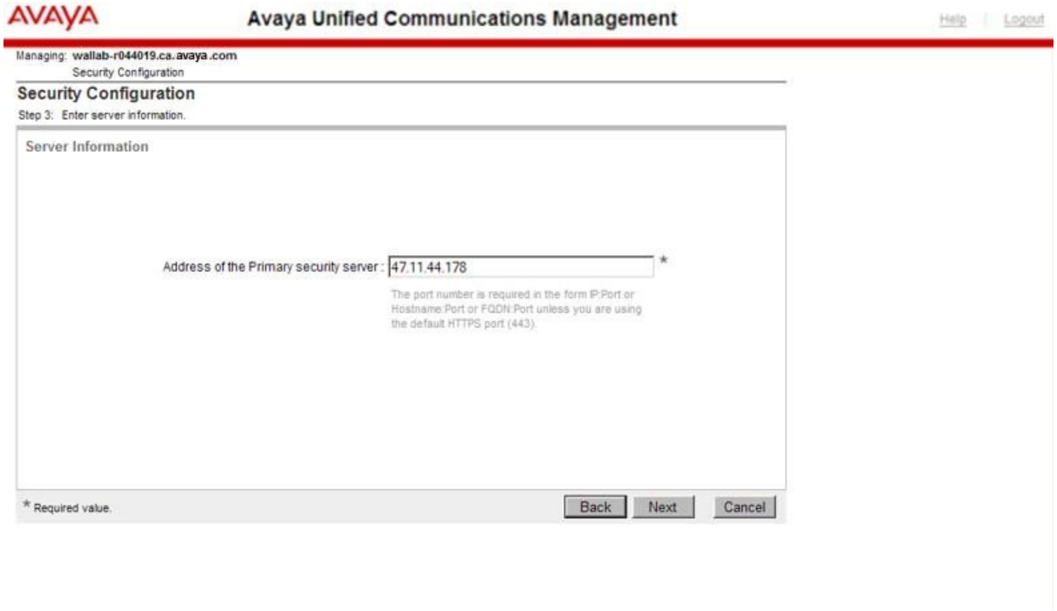
Managing: wallab-r44150.ca.avaya.com
Security Configuration

Security Configuration
Step 2: Select server type

Server Time : Fri Mar 13 17:21:03 EDT 2009

Server Type: ● Member server
○ Primary security server
○ Backup security server

3. Select the **Member server** radio button and click **Next**. The **Enter server information** page appears.



Managing: wallab-r044019.ca.avaya.com
Security Configuration

Security Configuration

Step 3: Enter server information.

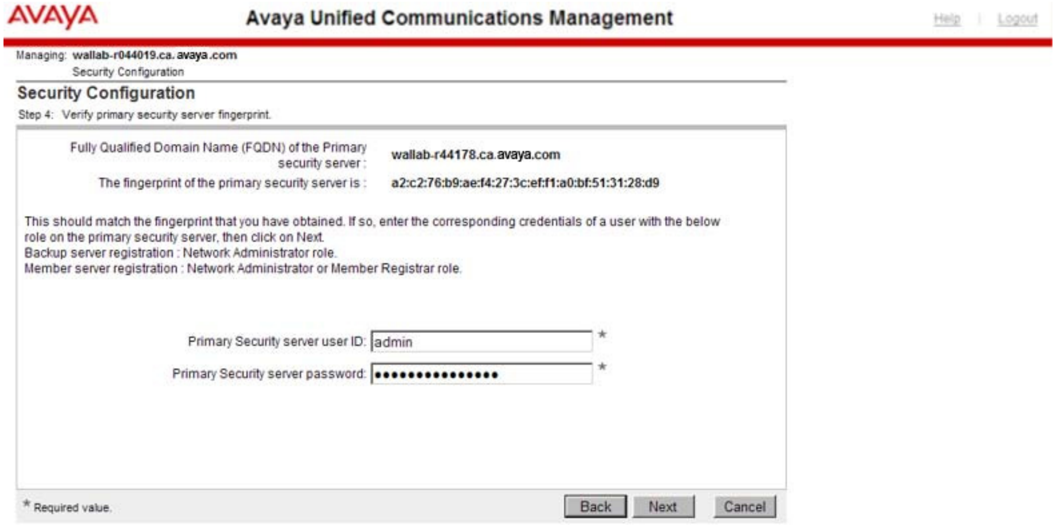
Server Information

Address of the Primary security server : 47.11.44.178 *

The port number is required in the form IP:Port or Hostname:Port or FQDN:Port unless you are using the default HTTPS port (443).

* Required value.

4. Enter the (TLAN) IP address of the Primary security server and click **Next**. The **Verify primary security server fingerprint** page appears.



Managing: wallab-r044019.ca.avaya.com
Security Configuration

Security Configuration

Step 4: Verify primary security server fingerprint.

Fully Qualified Domain Name (FQDN) of the Primary security server : wallab-r44178.ca.avaya.com

The fingerprint of the primary security server is : a2:c2:76:b9:ae:f4:27:3c:ef:f1:a0:bf:51:31:28:d9

This should match the fingerprint that you have obtained. If so, enter the corresponding credentials of a user with the below role on the primary security server, then click on Next.
Backup server registration : Network Administrator role.
Member server registration : Network Administrator or Member Registrar role.

Primary Security server user ID: admin *

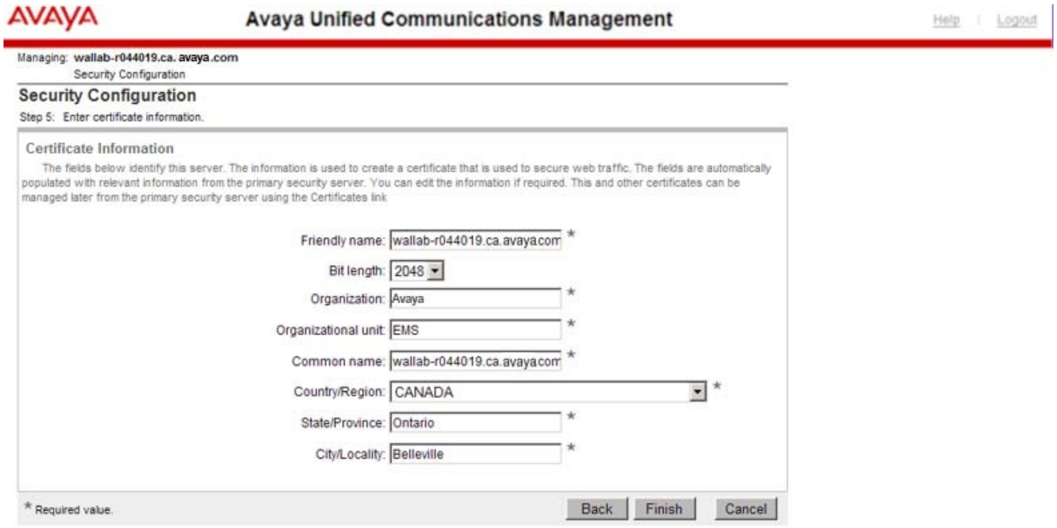
Primary Security server password: ●●●●●●●●●●●●●●● *

* Required value.

5. Verify that the FQDN and fingerprint information for the primary security server is valid and enter the following into the appropriate fields:

- Primary security server user ID (a UCM user ID with Network Administrator role)
- Primary security server password of the above user ID

6. Click **Next**. The **Enter certificate information** page appears.



Managing: **wallab-r044019.ca. avaya.com**
Security Configuration

Security Configuration

Step 5: Enter certificate information.

Certificate Information

The fields below identify this server. The information is used to create a certificate that is used to secure web traffic. The fields are automatically populated with relevant information from the primary security server. You can edit the information if required. This and other certificates can be managed later from the primary security server using the Certificates link

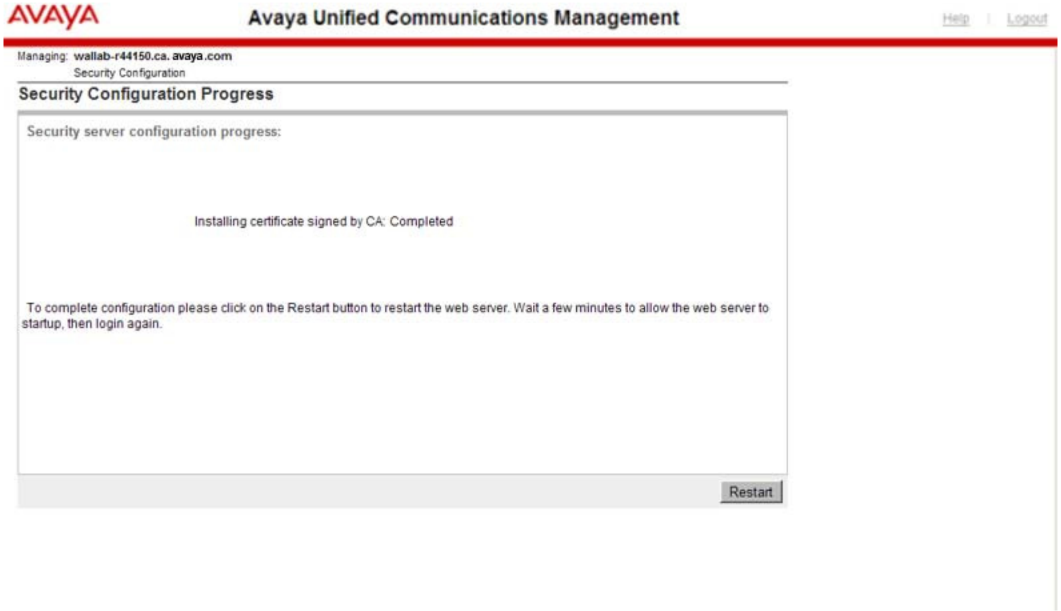
Friendly name: wallab-r044019.ca.avaya.com *
Bit length: 2048
Organization: Avaya *
Organizational unit: EMS *
Common name: wallab-r044019.ca.avaya.com *
Country/Region: CANADA *
State/Province: Ontario *
City/Locality: Belleville *

* Required value.

7. Enter the following information into the appropriate fields:

- Friendly name: A string to identify the certificate
- Bit length: Number of bits (512, 1024 or 2048) in the key used for encryption
- Organization: Your company name
- Organizational unit: A division within your company
- Common name: FQDN of the member server
- Country/Region: The country where the member server is located
- State/Province: The state/province where the member server is located
- City/Locality: The city/locality where the member server is located

8. Click **Finish**. The **Security Configuration Progress** page appears.



Managing: **wallab-r44150.ca. avaya.com**
Security Configuration

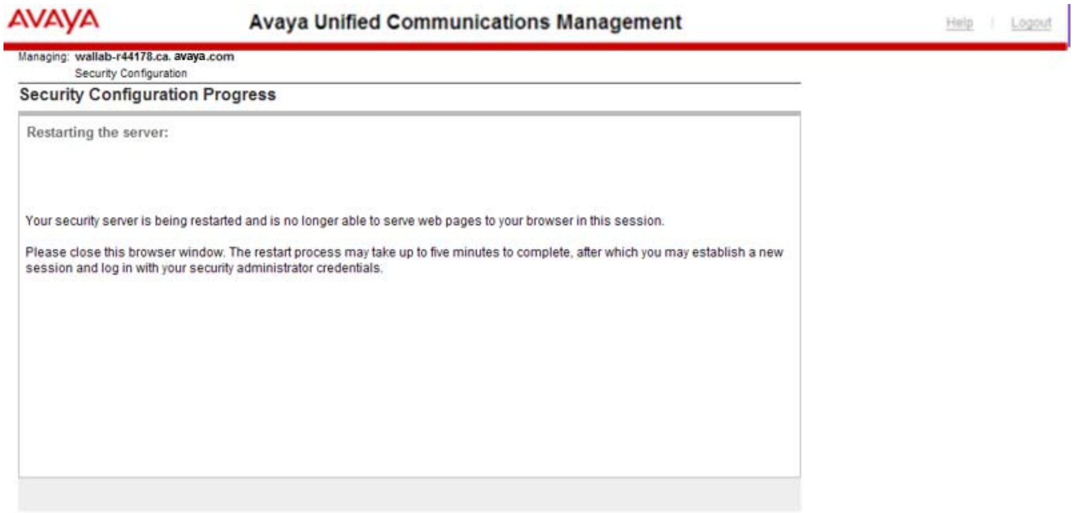
Security Configuration Progress

Security server configuration progress:

Installing certificate signed by CA: Completed

To complete configuration please click on the Restart button to restart the web server. Wait a few minutes to allow the web server to startup, then login again.

9. To complete the configuration process, you must restart the web server. Click **Restart**. The **Security Configuration Progress** page confirms that the server is restarting.



AVAYA
Avaya Unified Communications Management
Help | Logout
Managing: wallab-r44178.ca. avaya.com
Security Configuration

Security Configuration Progress

Restarting the server:

Your security server is being restarted and is no longer able to serve web pages to your browser in this session.

Please close this browser window. The restart process may take up to five minutes to complete, after which you may establish a new session and log in with your security administrator credentials.

The restart process may take up to 5 minutes to complete, after which you can establish a new session and log in with your security administrator credentials.

Note: If the Call Server needs to be accessed from a Linux-based server, there are three ways to do so:

1. If the Linux-based server is a UCM server only, the Call Server can be accessed by using **ssh**.
2. If the Linux-based server is configured to run any of the Signaling Server applications, the Call Server can be accessed by using **cslogin**.
3. If the Linux-based server is configured as a co-resident Call Server / Signaling Server system, the Call Server can be accessed by using **cslogin** or **csconsole** after successful activation of the Signaling Server. If the Call Server needs to be accessed before the activation of the Signaling Server to perform a new system installation, access is performed using **csconsole**.

Security Domain Users

The section titled “User and Password Management” in the *Security Management Fundamentals, NN43001-604* document contains a detailed description of the users and their associated privileges as well as their capabilities. The *Unified Communications Management Common Services Fundamentals, NN43001-116* document discusses in greater detail the roles that can be assigned to a user account and how to assign them to users.

Prior to registration with the security domain, the CS1000 Call Server and its elements will use the Call Server Level 1 account (PWD1 or ADMIN1), Level 2 account (PWD2 or ADMIN2), and PDT Level 2 account (PDT2) as system accounts; this includes the Signaling Servers and Voice Gateway Media Cards which are updated when EDD is run from LD 43.

After registration with the security domain, the CS1000 login accounts are suppressed and user login accounts will now be administered through the security domain. For more information, see the documentation referenced above.

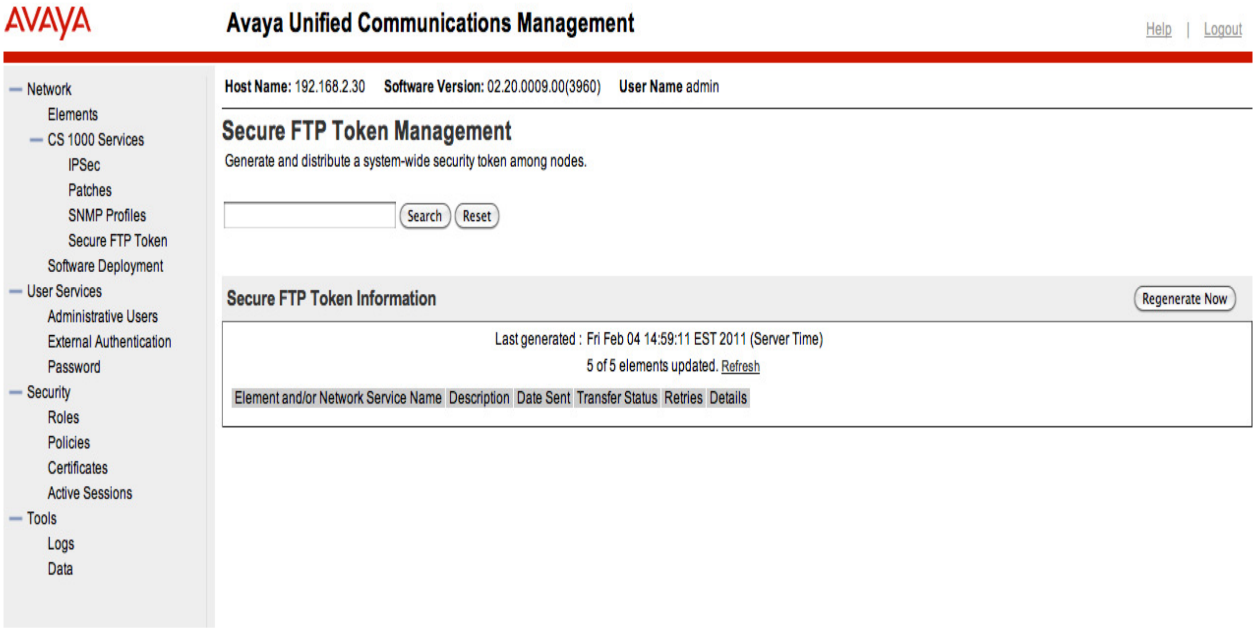
Note: Avaya strongly recommends documenting and storing the original CS1000 account passwords (ADMIN1, ADMIN2, PDT1 and PDT2) as they will be required for use in the event the CS1000 leaves the security domain.

Note: The ADMIN1, ADMIN2, PDT1 and PDT2 account names should not be used in the security domain account database. This would cause a conflict in security settings for these accounts, and may impact user capabilities.

The UCM account passwords follow the policies detailed in the *Unified Communications Management Common Services Fundamentals, NN43001-116* document. It must be noted that when a Call Server password expires, a warning message will **not** be displayed on the CLI and the password cannot be changed. If the password expires, you will see an invalid logon message when attempting to log in to the Call Server. At this point, the account is locked and the network administrator **must** reset the user account password.

Troubleshooting

On the UCM security server, the **Secure FTP Token Management** page can be used to validate a successful registration. Clicking **Regenerate Now** will recreate and distribute the secure token to all elements in the security domain. Check that there are no failures.



Avaya Unified Communications Management

Host Name: 192.168.2.30 **Software Version:** 02.20.0009.00(3960) **User Name** admin

Secure FTP Token Management

Generate and distribute a system-wide security token among nodes.

Secure FTP Token Information

Last generated : Fri Feb 04 14:59:11 EST 2011 (Server Time)

5 of 5 elements updated. Refresh

Element and/or Network Service Name	Description	Date Sent	Transfer Status	Retries	Details

The UCM security server log file in the /var/log/Nortel/Jboss-Quantum/log directory can also be used to monitor registration activity. To see the latest entries in the log, use the command:

- **tail –f** server.log

On the Call Server, the date/time of token creation/distribution can be viewed by going into the PDT/LDB shell and listing the /e/sdm directory. The date/time should match what is shown on the UCM security server.

To have all elements join a security domain successfully, each element has to be uniquely identified and have an individual ssh key. To verify if this is the case for a particular element, the baseOS properties file can be viewed and the field elementID should contain the specific FQDN of that element. If the elementID entry is similar to **elementId=localhost.localdomain** then it requires changing.

Also, the following commands may be useful in checking the status of security domain registration and other relevant items:

- **stat ucm sys**: Display list of elements associated with this Call Server and their registration status
- **stat ucm info**: Display IP address and fingerprint of UCM primary security server
- **stat transfers sec**: Check the status of secure transfers
- **ssh key show**: Display SSH keys

If an MGC, VGMC or MC fails to join the security domain via commands issued from the Call Server, use the CLI command **joinSecDomain** from the device itself.

If SSH keys need to be cleared and re-generated, follow these steps:

- **resetCAUTH**: Enable login using previous ADMIN2 credentials. (If the ADMIN2 password was changed from its default value, it needs to be reflected in UCM by editing the Call Server link.)
- **unreg ucm sys**: Remove elements from the security domain
- **ssh key show**: Display the current SSH keys
- **smCreateDefaultFilesAndData**: ****CAUTION**** Defaults all keys in the secret manager file. Enables a fresh attempt.
- **sshKeyGenerate** / **ssh key generate active**: Create new SSH key (may take up to 5 minutes)
- **ssh key show**: Display the newly-created SSH keys

The SSH debug commands on the Call Server and MGC are:

- **FCDebug=1**
- **sshDebug=1**
- **sshClientDebug=1**
- **SSHClientDebug=1**
- *<command>*= 0 will disable the given debug command.

These commands should be used with caution – the output is very large and processor-intensive. **Do not leave running.**

These are some tips on dealing with common errors that may be encountered when accessing EM:

- Keyfile error: Usually indicates a delay in the network – refresh the page a few times and check network connectivity
- PBXLink does not start: Usually seen after a node synchronization – restart applications from the Node Properties page
- EM will not synchronize node properties: Usually caused by a mismatch of secure FTP tokens (indicators can be found in the /var/log/nortel/ss_common.log file) -- regenerate tokens
- All EM access fails – Re-register the Call Server to the security domain, and check that the secure FTP token is updated.

Patches

Linux-based servers can be patched via CLI or GUI. There are two basic types of patches for these servers:

- Service Update (SU), which is an individual patch
- Service Pack (SP), which is a bundle of SUs

Each CS 1000 release may require the installation of specific service updates, loadware updates and/or service packs. As this list varies constantly, it is recommended that when installing the CS 1000 that the most current service updates, loadware updates and/or service packs applicable to the release be downloaded from the ESPL site which can be accessed at the following link: https://espl.avaya.com/espl/. A valid user name and password is required to access the site. The document titled *Enterprise Voice Solutions Patch Reference and Best Practice Guidelines* provides detailed information.

For each release, an installation bulletin is available and provides detailed information on the various steps to take in order to successfully install patches. The service updates titled cs1000-linuxBase-x.xx.xx.xx-xx, cs1000-baseWeb-x.xx.xx.xx-xx and cs1000-patchWeb-x.xx.xx.xx-xx, if present, must be individually installed on each server **before** installing any other service pack or service update. Refer to each bulletin for the latest versions of service packs and/or service updates. These bulletins are updated only when new versions of LinuxBase, BaseWeb and PatchWeb are delivered.

The current bulletins are available at the following links:

- Release 6.0: https://espl.avaya.com/espl/CS1000_6_0_ServicePack_Apr5_2011.pdf
- Release 7.0: https://espl.avaya.com/espl/CS1000_7_0_ServicePack_Mar22_2011.pdf
- Release 7.5: https://espl.avaya.com/espl/CS1000r7_5_Dependency_List_Service_Pack_v2.pdf

Currently, service packs are posted as .zip files. After obtaining a service pack, the file extension must be changed to .ntl from .zip. Do not change any other portion of the file name; if changed, patching operations will fail.

Application of a service pack will deploy different patches depending on the applications that have been deployed. Therefore, service packs need to be applied after application deployment.

The sFTP (winSCP) and SSH (Putty) tools are useful for transferring patches. You can obtain them as free downloads from the web.

The UCM Patch Manager can be used to upload patches including those that need to be activated via CLI.

The patching directories are:

- /var/opt/nortel/patch: Place SUs here.
- /var/opt/nortel/patch/sp: Place SPs here.
- /var/opt/nortel/patchlibrary: This is where UCM stores SPs.

The patching commands are:

- **pload**: Load patches
- **spload**: Load service packs
- **pins**: Install patches
- **spins**: Install service packs
- **pstat, spstat, issp**: Patch status

Also, the following commands may be useful for getting a snapshot of server status before and after patching:

- **swVersionShow**: Show application versions and deployed applications
- **appstart status**: Show which applications are running
- **ps –ef**: Show the task list.

Security Domain Checklist

The following is a quick list of key points from this document:

- Ensure the latest available patches are installed on all systems.
- If DNS is used, configure DNS first.
- Install and configure the primary (and backup if used) UCM security servers before other elements, and ensure that they are fully patched.
- Note that the FQDN of a UCM security server is associated with its TLAN IP address. In other words, the security server should always be configured using the TLAN.
- The PC used for web browser access to UCM should be connected to the TLAN.
- Ensure that all elements can reach the UCM security server(s), by configuring static routes if needed.
- Register VxWorks-based servers and devices via the ELAN. A CLI (telnet, rlogin or ssh) connection is needed for this.

- Register Linux-based servers via the TLAN.
- Use the Secure FTP Token Management page to validate successful registration.
- The “Troubleshooting” section in this document provides some tips for resolving issues if they come up.

Appendix A: Security Domain FAQ

1. **What should be done if the XML file is not received from the CS for a newly added IPMG?**
   Secure File Transfer must be disabled when installing a new IPMG to allow the XML file to download. The reason for this is because the new IPMG is not in the security domain. Once the XML file is downloaded Secure File Transfer can/should be re-enabled. Note that this procedure only applies to new installs.

2. **Which IP address (ELAN or TLAN) should be used to register a node to the security domain?**
   As referenced in the ELAN/TLAN Usage section:.
   - VxWorks elements (such as MGCs, MGSs, VGMCs, MC32s, MC32Ss, and Call Servers which are not on co-resident Call Server / Signaling Server systems): ELAN IP address
   - Linux elements (such as Signaling Servers, and co-resident Call Server / Signaling Server systems and the Call Servers on these systems): TLAN FQDN or IP address

3. **Which IP address (ELAN or TLAN) should be used to access the UCM security server?**
   As referenced in the ELAN/TLAN Usage section:
   - PC used for web browser access to UCM: TLAN (except in the case of the Managed Services configuration).
     - If a DNS is not in use the PC hosts file should include an entry containing the TLAN IP address and FQDN of the primary security server.
   - SNMP Access: ELAN

4. **If there are multiple ELAN subnets how should the communication be configured between the UCM security server and the elements residing on the ELAN subnets?**
   If a network has multiple ELAN subnets, static routes must be created to ensure communication between the UCM security server and the elements residing on the ELAN subnets.

5. **What should I do if multiple ELANs cannot be made routable or extended to set up communication between the UCM security server and the elements residing on the ELAN subnet?**
   For each of the ELAN subnets, a separate UCM security server is required. As mentioned in the ELAN/TLAN Usage section, UCM needs to be capable of communicating to all of its elements either located on the ELAN or the TLAN.

6. **If the wrong IP address is used when configuring a node to join the security domain (ELAN vs. TLAN) how can the configuration be corrected to allow the node to join the security domain?**
   It is possible to make the correction without redeployment. Refer to the procedure outlined in the “Security configuration changes” section on p. 74 of NN43001-116 (R6).

7. **Are there any Release 6.00R patches specifically written for security domain issues?**
   There are several including those listed below. Note that it is recommended that the current GA service patches and deplist be applied for all upgrades. As well, refer to PCN1787P for the recommended MGC loadware to be applied.

   MPLR30845 (Core): When attempting to join multiple MGC devices attached to the Call Server some get registered and some remain unregistered. This patch is a replacement for MPLR30184 and is included in the latest 6.0 Deplist .

   MPLR30611 (MGC): If the mgcdb.xml file fails to transfer from the CS to the MGC at MGC startup, the DSPs will not come up. This patch will try to use a local copy of the mgcdb.xml file if this happens. This is included in Loadware MGCCAP06 and above.

   NOTE: Rebooting the MGC has fixed several issues with the transfer of the mgcdb.xml file in the past. However:
   - IF THE MGC REBOOTS CONINUOUSLY WITH THIS MPLR APPLIED, it probably means that the local copy of the mgcdb.xml file on the MGC in /u/db is corrupted. Delete the file from the MGC using the rm command. If this stops the MGC from rebooting, it means that SFTP/FTP from the Call Server is failing and needs to be investigated.

   - If the MGC continues to reboot even after the mgcdb.xml file is removed from the MGC, the mgcdb.xml file on the Call Server is corrupted. Delete the file from the Call Server, and then reconfigure the MGC in the Call Server’s Element Manager.

MPLR30804 (CPPM): This is a *DEBUG* patch to release stuck SSH sessions. The symptoms reported include:

1. Cannot join any devices to security domain
2. Caused MGX/MGC to go into stuck state – manually leaveSecDomain on each one
3. Cannot Sync Node Properties
4. Cannot transfer mgcdb.xml properly

nortel-cs1000-Jboss-Quantum-7.00.20.10-04 (All Linux): Addresses the issue where the user that is not set to network administrator and attempt to access EM I get a WEB3610 message". Note that this patch is included in the latest SU.

8. **Is there a procedure for changing the IP address of the primary security server?**
The key part of changing an IP address is that the new Primary IP address must be known to all the existing backup/member servers prior to security domain registration.

If external DNS is used:

1. Ensure the DNS is changed to reflect the new IP address mapped to the primary security server's FQDN.
2. All the servers (including the primary/backup/member) must NOT have the mapping to the old IP in local /etc/hosts or C:\WINDOWS\system32\drivers\etc\hosts file.
3. Reboot the backup/member servers.

If external DNS is not used:

1. All the servers (including the primary/backup/member) must reflect the new IP address mapped to the primary security server's FQDN in local /etc/hosts or C:\WINDOWS\system32\drivers\etc\hosts file. This can be done in the Base Manager GUI (DNS and Hosts) or hostconfig cli.
2. Reboot the backup/member servers.

This procedure is documented in the NTPs for releases 7.00Q and 7.50Q (NN43001-260) but is not included in the Release 6.00R NTPs.

9. **Registration of an MGC to the security domain fails with SEC102: Failed to request membership in SEC DOMAIN. Reason failed Auth Open Flag. How is this addressed?**
If the LD 117 does not work then the next step is to log into the MGC and run the joinSecDomain command.

Appendix B: Static IP Route Configuration

Table B-1 summarizes the configuration of static IP routes for the Normal configuration pictured below:

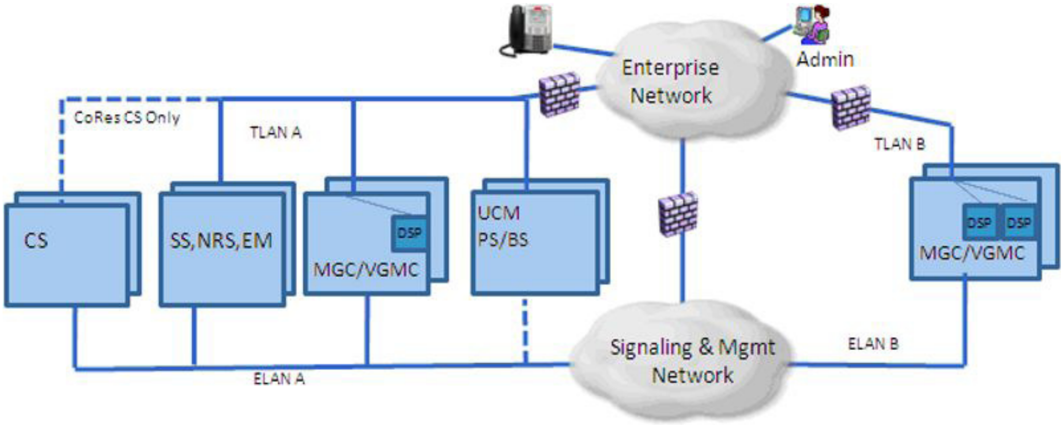


Table B-1: Static IP Route Configuration for Normal Configuration

Element Type (For Linux elements, this is based on UCM role -- primary, backup, member – and Deployment Manager packages)	**Destination(s)**	**Comments**
UCM Primary, UCM Backup		Default TLAN route is used
HA CS (VxWorks) (Created using LD 117 commands)	All (0.0.0.0/0)	Only a single network interface therefore default route can be used, but must be configured.
Co-Res CS (Linux)	ELAN addresses of MGCs, VGMCs, GR CSs, EM, SSs, SIPLs, TM, CallPilot, and Contact Center.	If using the AML Link splitting feature on a co-resident SS, routing to applications using this interface may not be required. Default route is via TLAN.
EM (Created using Linux Base Manager)	ELAN addresses of Call Server and dependent elements (CS, MGC, VGMC, SS and SIPL)	Default route is via TLAN.
Signaling Server, SIPL (Created using Linux Base Manager)	ELAN address of EM, ELAN address of VGMCs in same IP telephony node	Default route is via TLAN.
MGC (Created using Element Manager)	ELAN address of EM, FQDN address of UCM Backup	Default route is via TLAN.
VGMC (Created using Element Manager)	ELAN address of EM, FQDN address of UCM Backup	Default route is via TLAN.

Table B-2 summarizes the configuration of static IP routes for the Managed Services configuration pictured below:

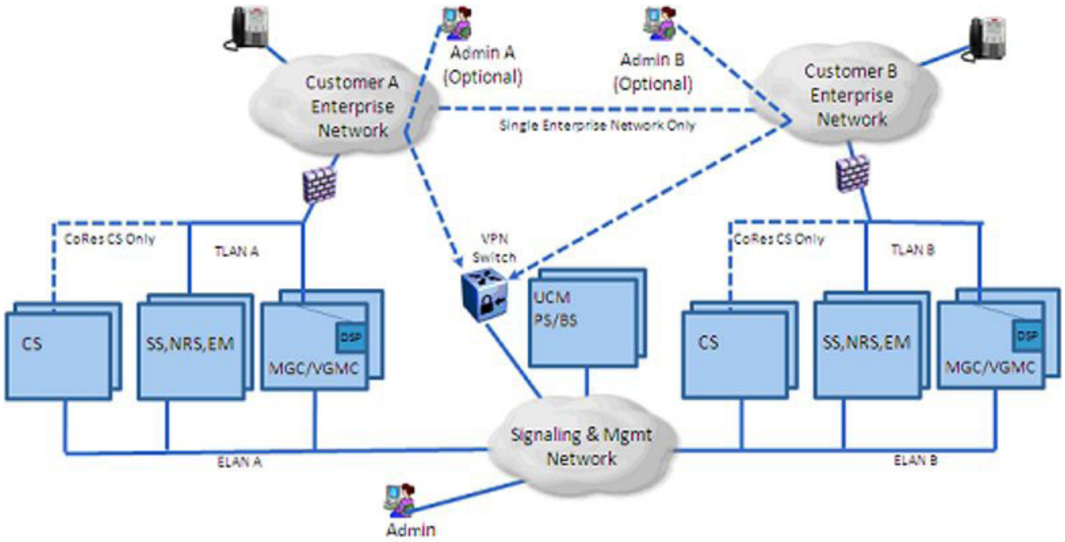


Table B-2: Static IP Route Configuration for Managed Services Configuration

Element Type (For Linux elements, this is based on UCM role -- primary, backup, member – and Deployment Manager packages)	**Destination(s)**	**Comments**
UCM Primary, UCM Backup	ELAN addresses of all members of the security domain (CS,EM, SS, VGMC, MGC, UCM Primary/Backup)	Network routes are recommended. Default route is via TLAN
HA CS (VxWorks) (Created using LD 117 commands)	All (0.0.0.0/0)	Only a single network interface therefore default route can be used, but must be configured.
Co-Res CS (Linux)	UCM Primary, UCM Backup, Management stations, and ELAN addresses of MGCs, VGMCs, GR CSs, EM, SSs, SIPLs, TM, CallPilot, Contact Center, VPN Switch subnet, 3rd Party Systems	If using the AML Link splitting feature on a co-resident SS, routing to applications using this interface may not be required. Default route is via TLAN.
EM (Created using Linux Base Manager)	UCM Primary, UCM Backup, Management stations, and ELAN addresses of Call Server & dependent elements (CS, MGC, VGMC, SS and SIPL), VPN Switch subnet	Default route is via TLAN.
Signaling Server, SIPL (Created using Linux Base Manager)	FQDN address of UCM Primary & UCM backup, ELAN address of EM, ELAN address of VGMCs in same IP telephony node	Default route is via TLAN.
MGC (Created using Element Manager)	ELAN address of EM, FQDN address of UCM Backup	Default route is via TLAN.
VGMC (Created using Element Manager)	ELAN address of EM, FQDN address of UCM Backup	Default route is via TLAN.

Appendix C: Security Domain Registration Commands for VxWorks

The following table shows the full list of commands that can be used to register, unregister and check registration status for VxWorks-based servers and devices:

Command	Type	Preconditions	Description
joinSecDomain	OAM/PDT CLI	• PWD2 privilege • Primary security server (ELAN) IP address • Username and password for a UCM administrator whose role includes Security Administration	Establish mutual trust with the primary security server.
leaveSecDomain	OAM/PDT CLI	• PWD2 privilege • Member of security domain	Remove the mutual trust information for the element.
statSecDomain	OAM/PDT CLI	• PWD2 privilege • Member of security domain	Display the primary security server IP address and fingerprint.
Register UCMSecurity CS	LD 117	• PWD1 or PWD2 privilege (R7.0 and higher); PWD2 privilege (R6.0) • Primary security server (ELAN) IP address • Username and password for a UCM administrator whose role includes Security Administration	Establish mutual trust with the primary security server for the Call Server. If the Call Server is already registered, it re-registers. (For co-resident Call Server / Signaling Server systems, this command only turns on central UCM authentication for the Call Server since the Call Server is registered as part of the overall system.)
Register UCMSecurity Device <ip_address>	LD 117	• PWD1 or PWD2 privilege (R7.0 and higher); PWD2 privilege (R6.0) • Primary security server (ELAN) IP address • Username and password for a UCM administrator whose role includes Security	Establish mutual trust with the primary security server for the element specified by <ip_address>, where <ip_address> is a Gateway Controller or VGMC registered to a Call Server belonging to the security domain.

		Administration	
Register UCMSecurity System [Force]	LD 117	• PWD1 or PWD2 privilege (R7.0 and higher); PWD2 privilege (R6.0) • Primary security server (ELAN) IP address • Username and password for a UCM administrator whose role includes Security Administration	Register all elements associated with this Call Server, such as Gateway Controllers and VGMCs, to the security domain after prompting for user approval. (If the system is a redundant system, the inactive Call Server joins the security domain automatically.) Use FORCE to request all elements to register, including those that are already registered (which will re-register).
Unregister UCMSecurity CS	LD 117	• PWD2 privilege	Remove the mutual trust information for the Call Server. (For co-resident Call Server / Signaling Server systems, this command only turns off central UCM authentication for the Call Server since the Call Server is registered as part of the overall system.)
Unregister UCMSecurity Device <ip_address>	LD 117	• PWD2 privilege	Remove the mutual trust information for the element specified by <ip_address>.
Unregister UCMSecurity System	LD 117	• PWD2 privilege	Remove the mutual trust information for the Call Server and all of its associated elements, such as Gateway Controllers and VGMCs.
Stat UCMSecurity Info	LD 117	• PWD2 privilege	Display the primary security server (TLAN) IP address and fingerprint.
Stat UCMSecurity	LD 117	• PWD2 privilege	Display all known elements (such as

System [Refresh]		Gateway Controllers and VGMCs) associated with this Call Server and their current registration status as Registered or Unregistered. Use REFRESH to refresh the list.