A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant/Manager

Webmin Base Administration

Administrator Documentation
11/2025

A31003-H34B0-M129-02-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

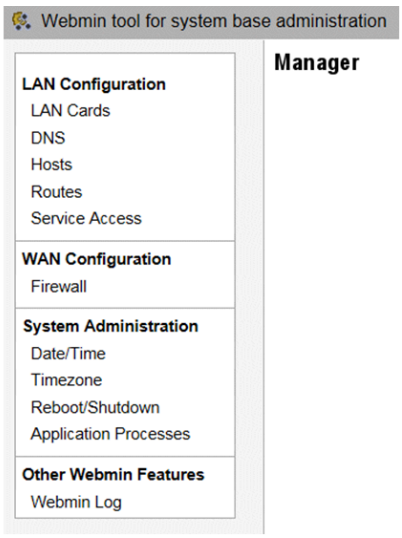
Contents

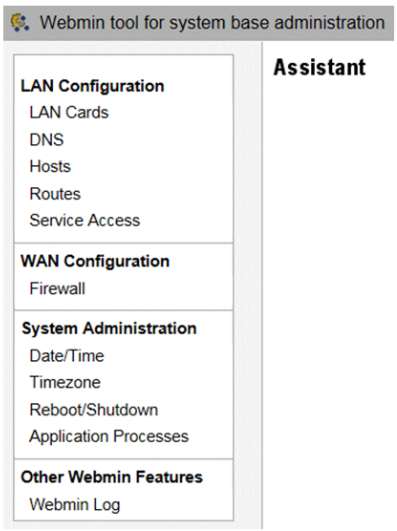
1 Overview

Webmin is the basic administration service for the configuration of the system resources and the TCP network on Linux. It is also used for operating the system, e.g. shutdown.

To start Webmin, select **Base Administration** -> **Webmin** from the **OpenScape 4000 Manager/Assistant** start page.

2 Home Page/Left Hand Navigation Frame





Functions Overview

LAN Configuration

- LAN Cards
- DNS
- Hosts
- Routes
- Service Access

WAN Configuration (Assistant only)

- Firewall

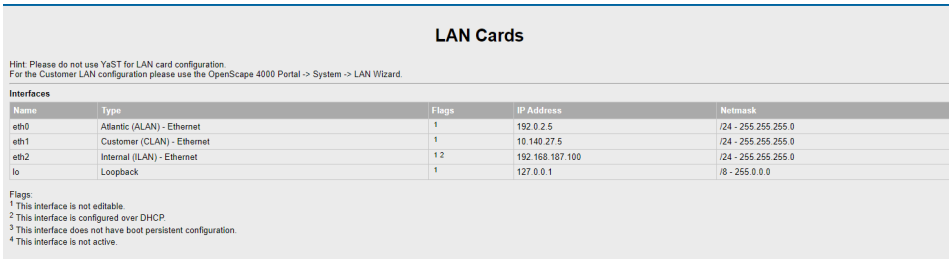
System Administration

- Date/Time
- Time Zone
- Reboot / Shutdown System
- Application Processes

Other Webmin Features

- Webmin Log

3 LAN Cards



LAN Cards

Hint: Please do not use YaST for LAN card configuration.
For the Customer LAN configuration please use the OpenScape 4000 Portal -> System -> LAN Wizard.

Interfaces

Name	Type	Flags	IP Address	Netmask
eth0	Atlantic (ALAN) - Ethernet	[1]	192.0.2.5	/24 - 255.255.255.0
eth1	Customer (CLAN) - Ethernet	[1]	10.140.27.5	/24 - 255.255.255.0
eth2	Internal (ILAN) - Ethernet	[1 2]	192.168.187.100	/24 - 255.255.255.0
lo	Loopback	[1]	127.0.0.1	/8 - 255.0.0.0

Flags:
[1] This interface is not editable.
[2] This interface is configured over DHCP.
[3] This interface does not have boot persistent configuration.
[4] This interface is not active.

On the **Assistant** the LAN card configuration is used to review the current configuration only.

In the **Type** column of the **Configured interfaces** table three kinds of networks are distinguished:

- ALAN
- CLAN and
- ILAN.

The Assistant checks its customer LAN address on the OpenScape 4000 portal during the Linux startup and reconfigures itself if a change has been made in the LAN Wizard.

NOTICE:

For OpenScape 4000 **Assistant**:

Do **not** use YaST for LAN card configuration, because this corrupts the config files!

When configuring the customer LAN card on the Manager you must specify an address within the customer LAN, assigned by the customer LAN administrator, and also a netmask and a broadcast address. On the Manager more than one LAN card may be configured.

The LAN card is configured and activated at the same time. After a reboot, all configured LAN cards are automatically enabled.

This chapter covers the following topics:

3.1 Parameters

- **Address**

  A unique address within the customer LAN must be assigned to each LAN card. This has to be defined by the customer LAN administrator.

- **Netmask**

  The netmask depends on the class of the LAN card address. For instance, for a class C address the netmask is 255.255.255.0. The netmask has to be defined by the customer LAN administrator.
- **Broadcast**

  The broadcast address is used to send datagram packets through the network, e.g. for address propagation from a router. The broadcast address depends on the LAN card address. For instance, for the LAN card address 218.100.200.204 the broadcast address can be 218.100.200.255. It is derived from the IP address of the LAN card and from the netmask.

3.2 Operations

NOTICE: Where not specified, the operation applies both to Manager and Assistant.

3.2.1 Activation of a LAN card

Configured LAN cards that are currently not active are marked with an asterisk.

- You can activate the LAN card, by clicking its name in the table of **Configured Interfaces**.

  After saving the interface configuration anew by clicking on the **Save** button and after confirming in a dialog box that the interface should be activated and that all services should be restarted, the interface activation will come into effect.

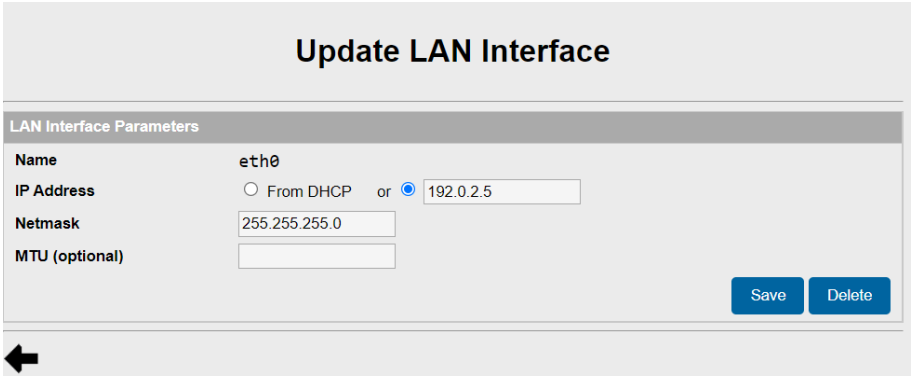
3.2.2 Deleting a LAN card (Manager only)

- You can delete a LAN card configuration, by clicking the particular LAN card name in the table and then pressing the **Delete** button on the **Update LAN Interface** page.

  The deletion will take effect immediately.

3.2.3 Adding virtual LAN interfaces (Manager only)

- You can add Virtual LAN Interfaces (Manager only) for an already configured LAN card, by clicking the **Add virtual interface** link on the **Update LAN Interface** page.



- When the **Add LAN Interface** page appears, enter **Name**, **IP Address**, **Netmask** and **Broadcast** in the corresponding fields.
- Click the **Create** button when you have completed your changes.

  The new virtual interface is activated immediately. You will be asked if you want to restart all services immediately in order to make them work with the new virtual interface.

  One or more virtual interfaces can be added to a real one, using the **Add virtual interface** link repeatedly.

3.3 Virtual LAN Interfaces (Manager only)

If you want to set multiple IP addresses for one LAN card you can add virtual LAN interfaces for this card (see Operations). "Virtual" means not separately present physically, but refers to an existing real interface.

3.4 Example

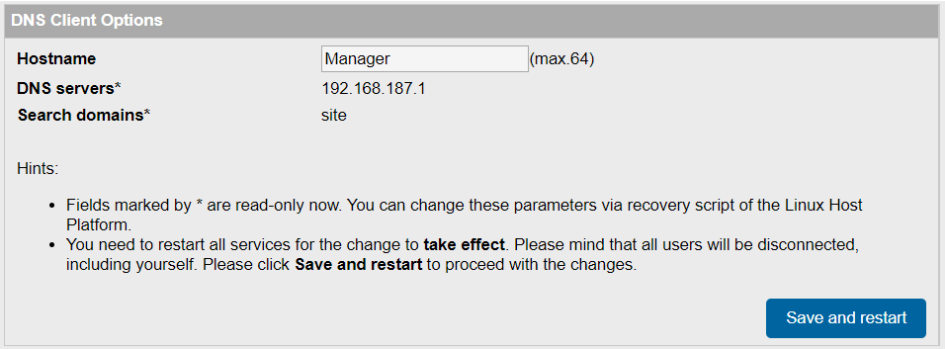
An unconfigured LAN card needs to be configured with an IP address, which is within the customer LAN's address range.

The following steps must be done:

1) Get an IP address within the address range of the customer LAN, e.g. 192.1.2.5.
2) Click the required LAN card name in the **Not configured interfaces** table.
3) Enter the LAN card configuration details in the **Add LAN Interface** page as follows:

   IP Address: 192.1.2.5 **Netmask**: 255.255.255.0 **Broadcast**: 192.1.2.255
4) Click on the **Create** button.

4 DNS



If the system is connected to a customer LAN where **D**omain **N**ame **S**ervice (DNS) is in use, then the server can be configured as a client to use that DNS service.

This chapter covers the following topics:

4.1 Parameters

- **Hostname**

  The host name is the name of this machine. This name is used by many of the networking programs to identify the machine.
- **Resolution order**

  Beside the Domain Name Service there are other name services like the Network Information Service (NIS) which can be used for name resolution. Resolution order determines which service should be used first and which thereafter. The first two services are fixed to Hosts and DNS, the three remaining can be set either to NIS or NIS+ or DB.
- **DNS Servers**

  Enter the IP address(es) of the DNS Servers provided by the Customer LAN administrator. There can be up to 3 DNS servers. To resolve a host name or IP address, the resolver initially asks the first DNS server and then sequentially the following DNS servers, until there are no more DNS servers available. In order to use DNS, at least one DNS server must be configured, the other two are optional. If no IP addresses are provided, then the Linux system will be configured not to use the DNS.

  On the **Assistant**, the DNS server address of the OpenScape 4000 portal is configured automatically by the DHCP. *Please do not change this configuration* if no problem in the DNS resolving occurs.

  If any of the LAN cards is configured to use the DHCP (see LAN Card Operations), the **DNS Servers** and **Search domains** may be configured by the DHCP.
- **Search domains**

  When the short name (without the domain suffix) of the host has to be searched, the resolver queries for the name relative to the domain names

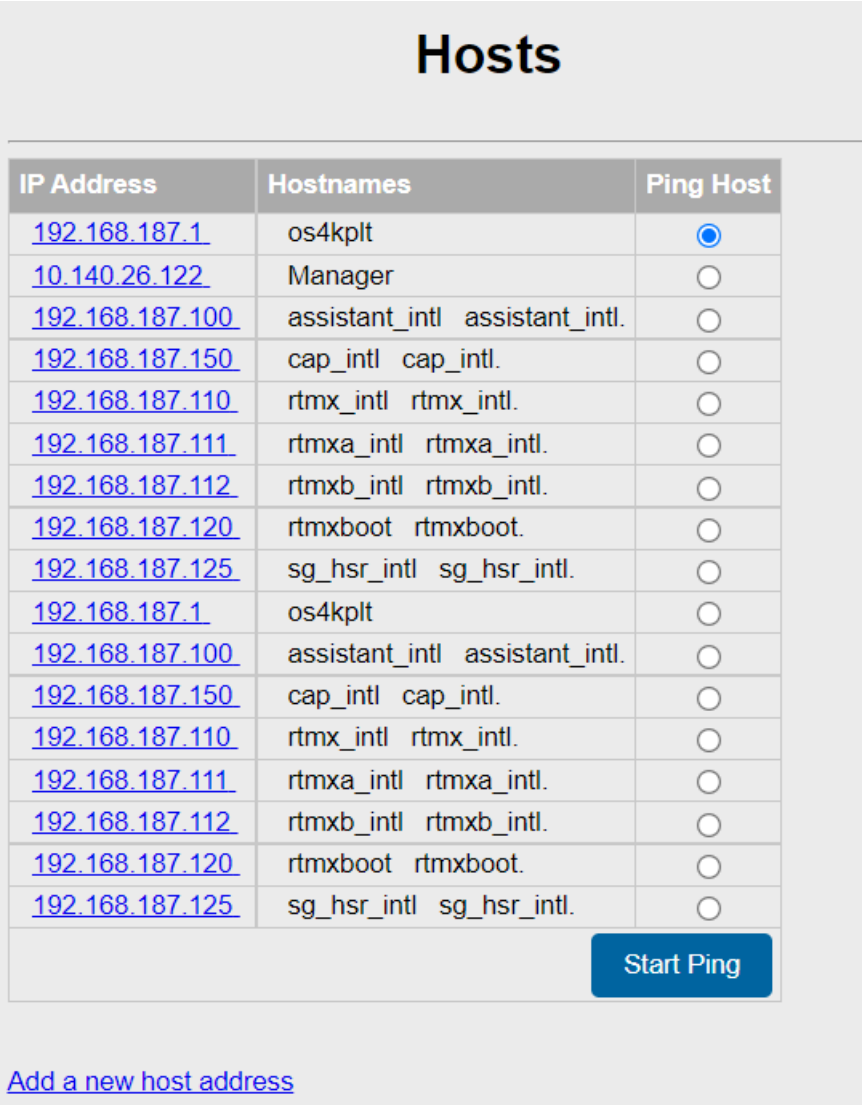
in the search list. If the **Listed** option is selected and a single domain is specified, it is considered to be local domain. If you wish to extend the search list, you can add more domain names in the **Search domains** field. The resolver will use each domain in the list until a match is found.

NOTICE: You will get the local domain name from the customer LAN administrator.

4.2 Operations

- You can **configure the Manager/Assistant to be a DNS client** by selecting the **Listed** option and typing the domain(s) name(s) in the **Search domains** field.
  - Define the DNS server(s) IP address(es) in the **DNS Servers** field.
  - You can specify additional name services in the **Resolution Order** fields.
  - Click on the **Save** button to perform the configuration.
- You can **remove** all domains by selecting the **None** option and clicking the **Save** button.
- To **stop using DNS**, delete all the server addresses and click the **Save** button.
- To **modify an existing DNS configuration**, alter the fields you wish to modify and click the **Save** button.

5 Hosts



This section shows the configuration of hosts in the /etc/hosts file. To configure a host, a name has to be mapped to the host's IP address, e.g. Pluto to 139.1.2.40. Then you can address the host by this name. Network routines (DNS resolver) use this host configuration data to translate between names and IP addresses.

This chapter covers the following topics:

5.1 Parameters

- **Hostnames**

  Each name must be unique. The name is a string with maximum 50 characters.

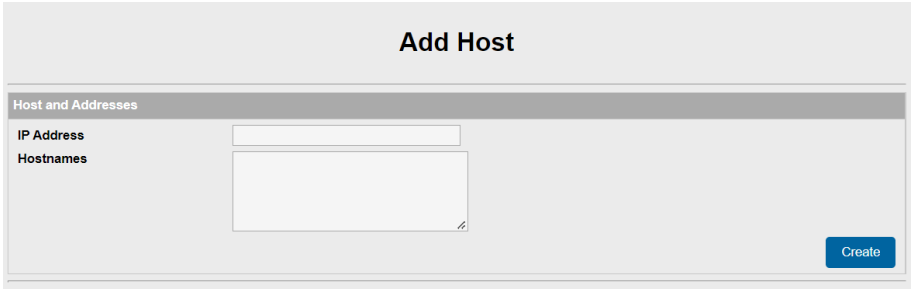
- **IP Address**

  The IP address of the host.

5.2 Operations

Adding a host

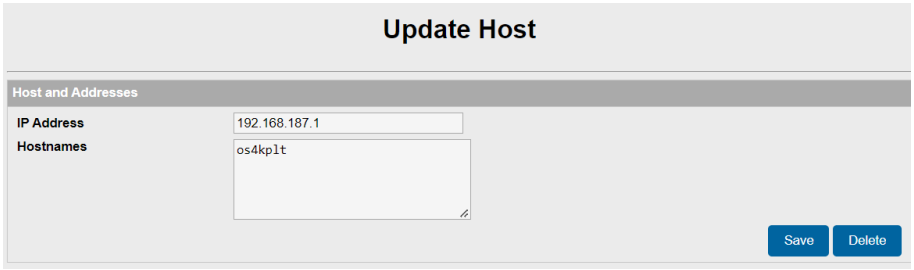
- You can **add** a host by clicking the **Add a new host address** link.



- Click the **Create** button, when all entries are complete.

Deleting a host

- You can **delete** a host by clicking its link under IP address on the **Hosts** page.



- Click the **Delete** button on the **Update Host** page.

> **NOTICE:** On the **Assistant** there are special default hosts configured which must not be removed! These are: ADP-RMX, WAML, ADP-UNIX, os4kplt, cap_intl.

- You can **ping** a host by selecting it on the **Hosts** page and then clicking the **Start Ping** button.

5.3 Example

For a host, connected to the customer LAN (e.g. Jupiter), a host name has to be configured.

Following steps must be done:

1) Get an IP address within the customer LAN, e.g. 191.1.2.6.

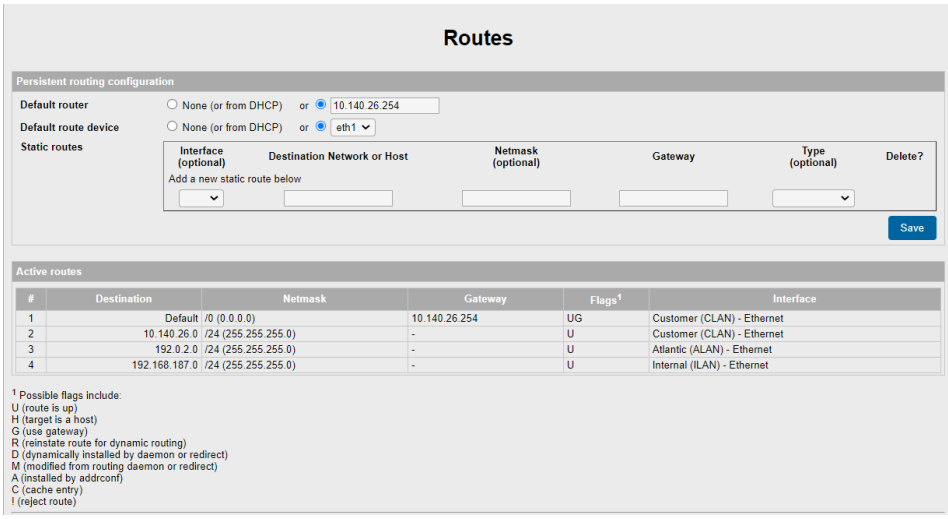
2) Add a host name as follows:

Name: Jupiter

Address: 191.1.2.6

3) Click on the **Create** button.

6 Routes



This section describes the configuration of routes, which are needed when exchanging data between hosts on different networks. Certain hosts, called "gateways", are responsible for exchanging routing information and forwarding data from one network to another until the data reaches its final destination.

The table in **Persistent routing configuration** displays only the static routes configured on the Linux. All active routes including dynamically configured routes (e.g. through DHCP) are displayed in the **Active routes** table.

There can be one default route configured which will be used if no other route matches. This default route defines the default gateway to which IP packets are forwarded.

NOTICE: For the Assistant, the default router is configured in the LAN Wizard on the OpenSape 4000 portal. Afterwards the configuration is done automatically on the Assistant. **Please change it here only in emergency cases.**

Routes can also have a netmask applied to them. This field is optional, and in most cases it should be left blank. Where there are complex routing requirements, it may be necessary to apply a netmask to a particular route. This can be used to create a route to a sub-netted part of the customer network.

This chapter covers the following topics:

6.1 Route Parameters

- **Interface**

  Enter a LAN interface in this field to force the route to be associated with the specified LAN interface (e.g. eth0), as the routing process will otherwise try to determine the device on its own. In usual networks you won't need this.

- **Network**

  The Network field specifies the destination host or network. For a host route the IP address of the host has to be specified. For a net route the network address has to be specified.
- **Netmask**

  This must be a value, which will "mask off" a certain part of the IP address of the destination field, creating a route to a sub-net which will use the gateway specified. It must have a value, which, when converted to binary consists of a number of digits 1s, followed **ONLY** by 0s (i.e. not mixed). An example is given in the Examples section.
- **Gateway**

  This field defines the IP address of the gateway. The gateway must be reachable.
- **Type**

  You can enter the route type in this field.

  The most often used types are the following:

  – **unreachable**

    Causes the destinations to be unreachable. Packets to this destination are discarded and the message "host unreachable" is generated.
  – **blackhole**

    These destinations are unreachable. Packets are discarded silently, i.e. no message is generated.
  – **local**

    The destinations are assigned to this host. The packets are looped back and delivered locally.
  – **broadcast**

    The destinations are broadcast addresses. The packets are sent as link broadcasts.

6.2 Operations

- You can **set a default route** manually by selecting the "or" option for the **Default router**. Fill in the IP address of the default gateway. You can also give the name of the **Default route device** when you select the option "or" for the **Default route device** field.
- You can set this host to act **as a router** for other systems by selecting the **Yes** option.
- You can **add** a route by filling the route parameters to the last row of the table. Click on the **Save** button when finished. The page reloads and you can add another route.
- To **modify** an existing route, alter the fields you wish to modify and click the **Save** button.

- You can delete a route by clearing all fields of a line in the table and a clicking the Save button.

  The configuration is saved but the changes will not take effect until you confirm the dialog box that appears after clicking the **Save** button.

  In this dialog box you will be asked to confirm the activation of the changes and the restart of all OpenScape 4000 Manager/Assistant services, to make them work with the new settings.

  – Click on the **Yes** button to activate the changes and to restart all services right away.
  – Click on the **No** button if you don't need to activate the changes right now.

    In this case, the activation will be done automatically after system reboot.

6.3 Examples

Example - Adding a host route

For a host, connected to the customer LAN (e.g. Jupiter), a host route has to be configured.

The following steps must be done:

1) Get an IP address within the address range of the customer LAN, e.g. 191.1.2.6 and the gateway address, e.g. 191.1.2.40.

2) Add the host route as follows:

Destination: 191.1.2.6

Gateway: 191.1.2.40

Example - Using a route with a netmask

If a customer requires a route to a sub-netted part of the LAN (e.g. 138.223.236.z) to use a gateway other than the default gateway, then normally adding a route of 138.223.236.0 would only provide a route to that individual host.

In order to make a net route to the sub-net 138.223.236.z range of addresses, a netmask of 255.255.255.0 must be applied. Determining the correct netmask value requires the detailed understanding of the customer's LAN and should only be done with the help of the customer LAN administrator.

The netmask value is used by taking the binary representation of its value and performing a bit-wise logical AND operation with a destination address (such as 138.223.236.9). This "masks off" the network part of the address - in this case the result of the netmask 255.255.255.0 being applied to 138.223.236.9 is 138.223.236.0.

The result of this operation is used to locate the correct gateway address from the routing table, i.e. the route to 138.223.236.0 which is the gateway 139.2.54.56 as required.

In this case the following steps must be done:

1) Get an IP address within the sub-netted part of the customer LAN, e.g. 138.223.236.0, the gateway address, e.g. 139.2.54.56 and the netmask value, e.g. 255.255.255.0 from customer LAN administrator.

2) Add the host route as follows:

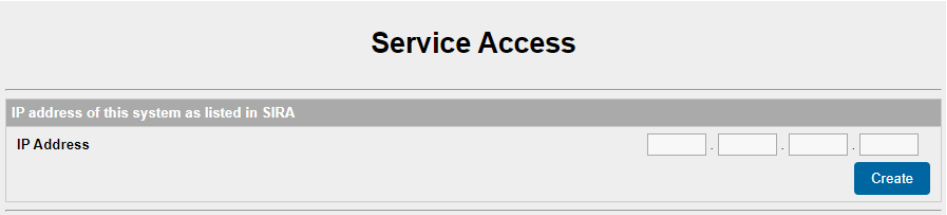
Network: 138.223.236.0

Gateway: 139.2.54.56

Netmask: 255.255.255.0

The route which has been added results in access to any IP address in the range 138.223.236.0 - 138.223.236.255 using the gateway 139.2.54.56 instead of the default gateway.

7 Service Access



The Linux system can be remotely administered using SIRA service access. In SIRA the system is assigned an individual IP address of the form 10.B.C.D. The B, C and D fields must be allocated specifically to this OpenScape 4000 Manager/Assistant by a service representative, and are based on the number of OpenScape 4000 Assistant servers.

The SIRA address is identical to the former VPN address. The VPN addressing structure is replaced by the SPoA/NAT concept.

This chapter covers the following topics:

7.1 Operations

- To **add** the SIRA IP Address, fill in the address and click on the **Create** button when finished. Please confirm the creation of the service access configuration by clicking the button **Create Service Access Configuration**. All services are restarted and all users are disconnected, including you.
- To **modify** an existing SIRA IP Address, alter the IP address fields and click on the **Modify** button. When you confirm the change(s) by clicking the **Modify Service Access Configuration** button, all services are restarted and all users are disconnected, including you.
- You can **delete** the SIRA IP Address by clicking the button **Delete**. Please confirm the deletion of the service access configuration by clicking the **Delete Service Access Configuration** button. All services are restarted and all users are disconnected, including you.

7.2 Example

On a OpenScape 4000 Manager/Assistant, which is directly connected to the RSP (Remote Service Platform), the SIRA address needs to be configured.

Assume that following address is given: 10.2.191.1

The following steps must be done:

1) Enter the SIRA IP address 10.2.191.1 in the address fields.
2) Click the **Create** button to create the service access configuration.
3) Click the **Create Service Access Configuration** button to confirm.

8 Firewall

8.1 Firewall on Manager

The Firewall page on Manager has mainly an informational character:

Overall Status

You can change only two options:

- SuSE firewall
- SuSE firewall automatic starting

You can switch on and off these options by using the respective buttons.

Important note: It is strongly recommended to **keep both options switched ON!**

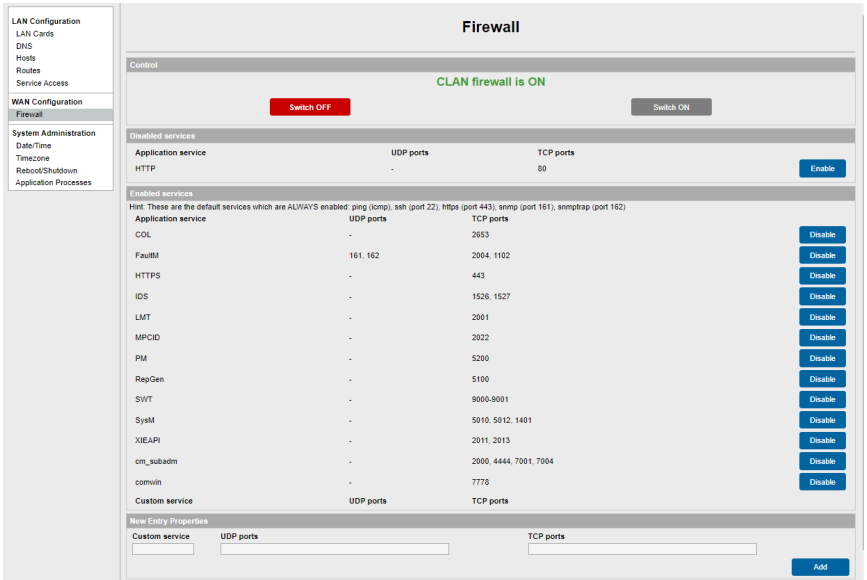
WARNING: Switching the SuSE firewall OFF is a security threat!

Firewall Interfaces

This part shows which interfaces are allowed for which zone.

Registered services for External Zone

This part shows which services and ports for these services are allowed for which zone.



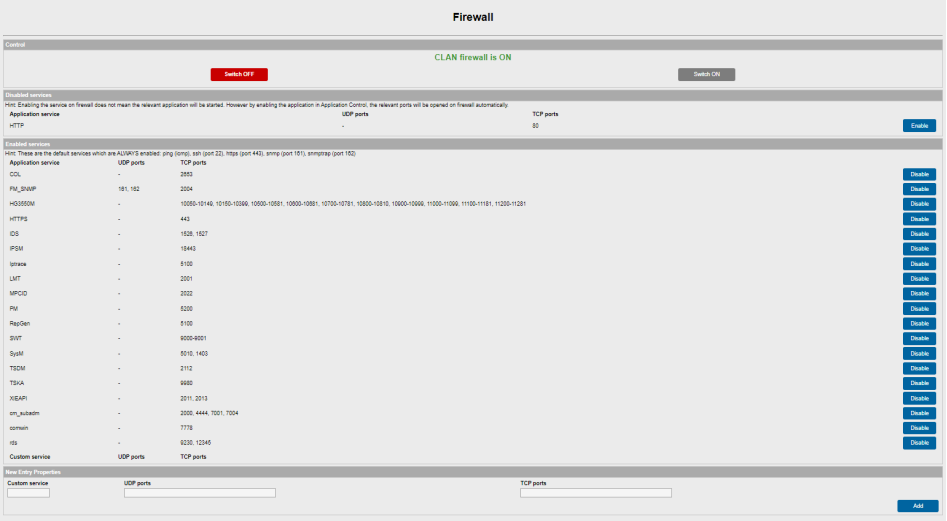
8.2 Firewall on Assistant

The Assistant firewall generally consists of the ALAN firewall (**A**tlantic **LAN**) and CLAN firewall (**C**ustomer **LAN**).

ALAN firewall

The ALAN firewall is an address filter, which forwards IP packets coming from the CLAN hosts to the ALAN hosts or ADP. Only those IP packets from CLAN hosts which have access rights are forwarded. All other IP packets are rejected.

When Secure Mode for ADP (Security Mode Configuration) is enabled, the access to ALAN and ADP is prohibited completely. All firewall allowed hosts are blocked and no host can be added or removed. This does not affect Comwin functionality because the Comwin goes a different way in Secure Mode.



CLAN Firewall

The table **Dynamically registered services on CLAN** is a summary for the CLAN firewall.

The CLAN firewall cannot be configured here. But according to the settings of Secure Mode (system shell from CLAN, remote ODBC/JDBC access, etc.) some ports can be closed, while still displayed in this table.

The user can switch the CLAN firewall ON or OFF.

WARNING: Switching the CLAN firewall OFF is a security threat!

Overview of the following sections:

- Access Rights
- Operations
- Example

8.2.1 Access Rights

The following access rights are defined:

- **ALAN**

  The individual host or the hosts on the net for which the Firewall Entry is defined are allowed to access all hosts on the ALAN, except the OpenScape 4000 Assistant itself.

- **ADP**

  The individual host or the hosts on the net for which the Firewall Entry is defined are allowed to access the RMX-ADP on the OpenScape 4000 Assistant.

One or more access rights can be assigned to a Firewall Entry. The superset of these access rights defines the allowed communication paths.

8.2.2 Operations

- To **add** the Firewall entry, specify the following:

  1) CLAN Host / Net:

  Enter the valid IP address of the host or network which is to be allowed.

  2) Netmask:

  Check **Access to ADP (ComWin)**.

  3) Click the **Add** button.
- You can **delete** a Firewall entry by clicking the **Delete** button beside the corresponding entry.
- You can **switch on and off** the CLAN firewall by clicking the **Switch ON** button and the **Switch OFF** button in the **Control** area.

  Note that switching the firewall OFF is a security threat!

  Switch ON button = Enable the CLAN firewall.

  Switch OFF button = Disable the CLAN firewall.

  The ALAN firewall can *never* be off.

8.2.3 Example

A host, e.g. Jupiter, connected to the customer LAN, needs access to the OpenScape 4000 (RMX-ADP) via LAN. To allow the communication between the OpenScape 4000 and the Jupiter host, a firewall entry for the Jupiter host has to be configured.

The following steps must be done:

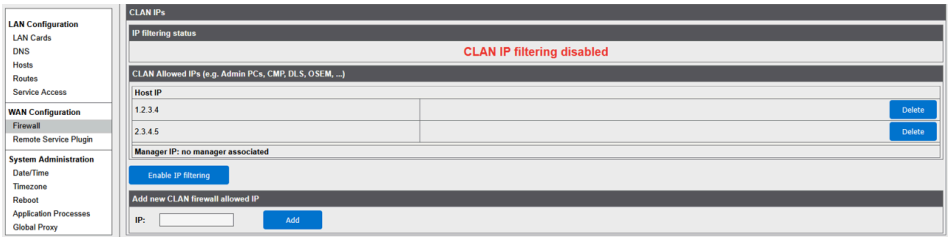
1) Get the IP-address for the Host within Customer LAN, e.g. 191.1.2.6.

2) Add a firewall entry as follows:

- Enter the IP address 191.1.2.6 in the **CLAN Host / Net** field.
- Click the **Add** button.

8.3 CLAN IP Filtering

Overview:



The CLAN IP Filtering feature offers the option to restrict access to Assistant/Manager by defining a list of IPs allowed to access the system. The IPs can be Admin PCs or other systems which need to communicate via CLAN with Assistant/Manager.

Operations:

- Enter a valid IP address and click **Add** to allow the system with the associated IP access to Assistant/Manager
- Delete an entry by clicking **Delete** beside the IP address. In order to prevent accidental lock-outs, this operation is only possible when the feature is **disabled**.
- Enable/disable the feature. Enabling the feature is only possible when at least one IP address has been added to the CLAN Allowed IPs list.

Additional information:

- If the system is an Assistant and it is connected to a Manager, the Manager IP is auto-filled in the CLAN Allowed IPs list.
- If the system is a Manager and it is connected to one or more Assistants, IPs of all Assistants are auto-filled in the CLAN Allowed IPs list.
- When enabling the feature existing sessions may continue to work even if the IP is not in the CLAN Allowed IPs list. New sessions will be refused.

IMPORTANT:

If you have configured an Admin PC in the IP address whitelist and this PC is not available anymore, or you have another situation where access is lost due to this feature, make a ticket and GPS will help you to unlock the firewall in Assistant/Manager.

---

9 Remote Service Platform

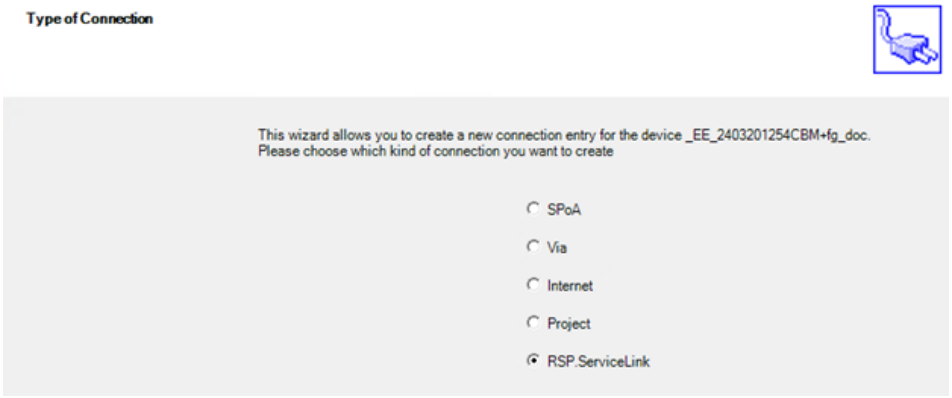
9.1 Overview

The RSP (Remote Service Platform) concept adds a new connection channel to the SIRA ecosystem, which is used by support for remote connections to customer systems. If until now a modem was used to establish a SIRA connection, now an OpenVPN tunnel is used which can be configured by the technician based on the SIRA profile. The only requirement now is an internet connection.

INFO: Initially SIRA was designed to use IP addresses from the 10.0.0.0/8 class. This range can often conflict with the customer's LAN subnet which could lead to routing issues. Now for the new RSP feature range 100.64.0.0/10 will be used. This range is globally reserved for tunneling and ISP address ranges, thus should not collide customer's LAN subnets. This IP addresses are not visible anywhere outside our RSP service.

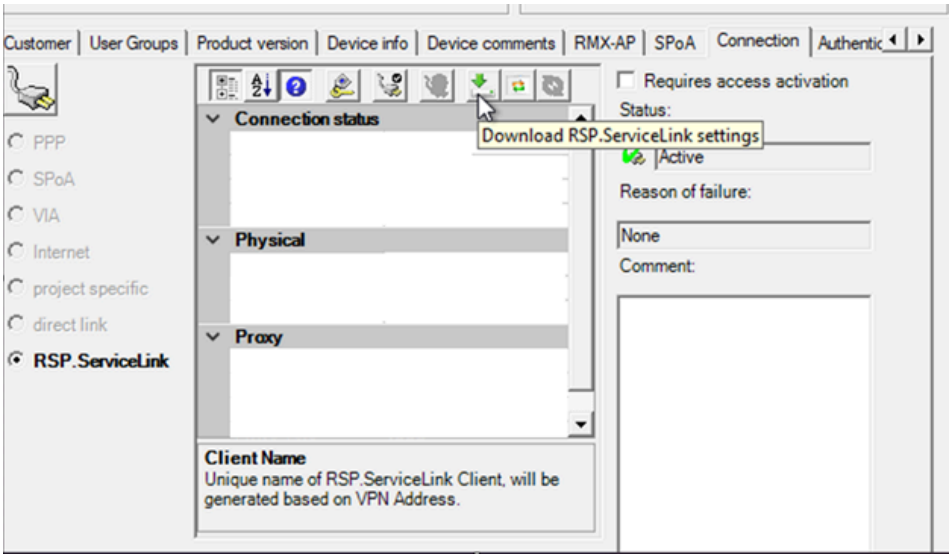
9.2 Configuration on SIRA

In order to configure the RSP option a new profile must be defined on SIRA with V11 and for the connection type RSP.ServiceLink must be selected.



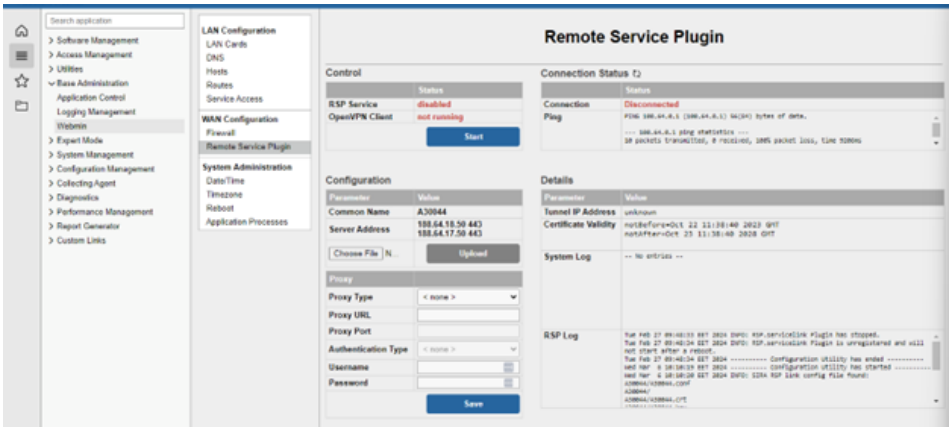
At the end of the Configuration Wizard the configuration tar file must be saved. This will be used on the system side to complete the configuration for this service.

In case the configuration tar file was not saved this can be downloaded from the system configuration entry, under the **Connection** tab, by selecting the **Download** button.

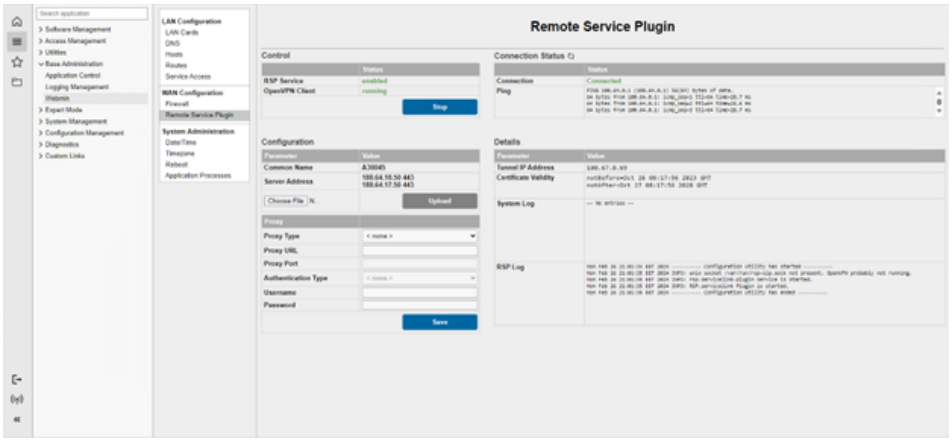


9.3 Configuration on OpenScape 4000

For this service a new entry was added under Webmin page called Remote Service Plugin. And in order to configure the service the tar file provided by the SIRA must be uploaded under the Configuration context menu. Once the configuration tar file is uploaded the service can be started. In case a proxy is required for the internet connection, the corresponding details must be provided as well.



Once the service is started and the connection is established this will be shown in the page by the corresponding status and color.



9.4 The configuration file

The configuration file will contain all the necessary certificates and keys for the OpenVPN connection to secure the tunnel between client and server. Therefore, certificates must be placed on both sides.

Certificates stored on the client side:

- client public crt
- client private key
- corporate CA chain

Certificates stored on the server side (SIRA):

- server public crt
- server private key
- RSP client CA chain
- RSP certificate revocation list (CRL)

When OpenVPN client connects to the RSP server, the key exchange is done. Both sides check the received certificates against their locally stored CA certificate chain. If they fit, they build up the tunnel. Client certificates are issued and signed by the RSP client Certificate Authority, while RSP server's certificates are signed by the Corporate (Unify) Certificate Authorities. So, every client has a copy of the corporate certificate chain, and every server has access to the RSP CA chain to check the client certificate against.

Unify Server 2015 CA

Unify Server 2015 CA is the currently used intermediate CA for RSP client connections, to make clients able to check, if they are connecting to an Unify signed OpenVPN server.

Certificates must be renewed every 3 years. CA certificate chains are stored on every client, which they can check the server certificate against.

RSP client CA

RSP client CA is an internal CA for being able to automatically manage RSP connection client certificates. Certificates are signed and revoked in sync with RSP device connection creations and deletions. Every deleted connection will send the certificate to the RSP Certification Revocation List, to reject further connections to the RSP.

Registrar CA

Used for automatic registrar. Automatic self-registration allows Assistant free configuration of the plugin, only using SIRA tools.

NOTICE: This sub-feature will be delivered later.

10 Date/Time

This section describes the configuration of the date, the time, the clock source and the update period.

The configuration of date and time for Manager and Assistant is handled differently:

- Date/Time Configuration for Manager
- Date/Time Configuration for the Assistant

10.1 Date/Time Configuration for Manager

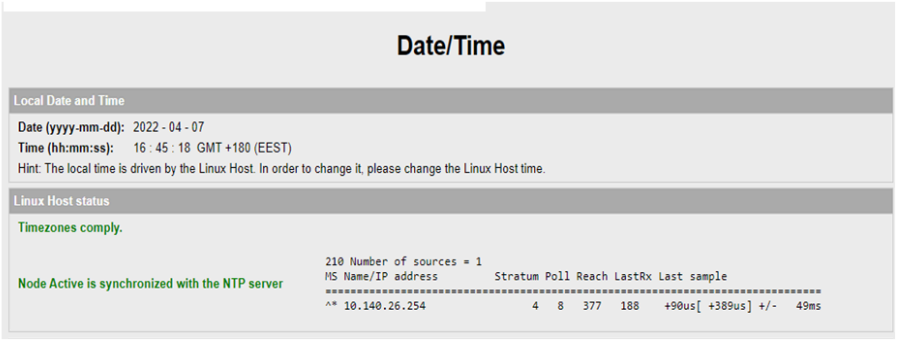
This section describes the configuration of the date, the time, the clock source and the update period for the OpenScape 4000 Manager.

General Information on Clock Source and Synchronization Status

- **External Time Server - Periodic Updates**

  When the clock source is configured to **EPU** mode (External Time Server - Periodic Updates) and a time server is configured, the table **Configured Clock Source** displays the details of the last synchronization attempt.

  This gives information that the Manager is synchronized with the external clock source.

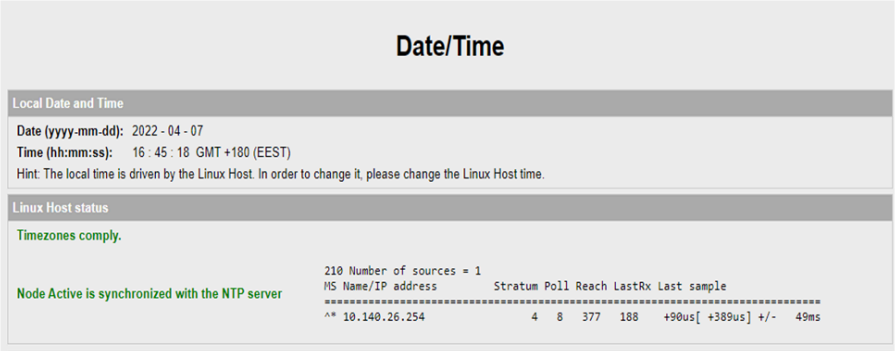


  The table shows: When the last synchronization attempt was made and with which NTP server (because there can be configured many NTP servers) sychronization was done, which action has been taken, and what is the overall status.

- **External Time Server - NTP Server for other Systems**

  The ENTP mode status table shows: Which servers are configured as the clock sources and what their roles in the NTP synchronization process are.

The Manager is synchronized to the server which is highlighted bold and has the role "Synchronized to".



The following server status are possible:

– Reachable

  Can be reached but is not synchronized yet, or is not a candidate for synch.

– Synchronized to

  To this server the system is synchronized.

– Unreachable

  This is not a NTP server or not accessible.

– Candidate

  Next candidate when the first server fails.

Related Topics

- Parameters
- Operation

To set the time zone for the system, please refer to section Time Zone.

10.1.1 Parameters

- **Configured Clock Source** The modes are:
  - **HW Clock - Standalone**

    Choosing this option:

    - The user may set the time for this system.
    - No other system may use this system as a time server.
    - This system will not seek time synchronization with any other system.
  - **HW Clock - NTP Server for other Systems**

    Choosing this option:

    - The user may set the time for this system.
    - Other systems may use this system as a time server.
    - This system will not seek time synchronization with any other system.
  - **External Time Server (Periodic Updates)**

    Choosing this option:

    - The user may not set the time for this system.
    - Other systems may not use this system as a time server.
    - This system will seek time synchronisation from a single configured time server system, starting at midnight and subsequently, after the configured **update interval**. An update period of about 2 hours should be adequate.
  - **Ext. Time Server - NTP Server for other Systems**

    Choosing this option:

    - The user may not set the time for this system.
    - Other systems may use this system as a time server.
    - This system will seek synchronization with the other configured time servers, using the Network Time Protocol.
- **Update Interval**

  Update Interval is relevant only when the clock source is **External Time Server (Periodic Updates)**.
- **Date (yyyy-mm-dd)**

  The format for the date is yyyy-mm-dd. For instance, 2010-01-22.
- **Time (hh:mm:ss)**

  The time is in 24 hour format. For instance, 14:23:05.
- **Time Server Name or Address**

  Please specify the name or IP address of external time server system.

10.1.2 Operation

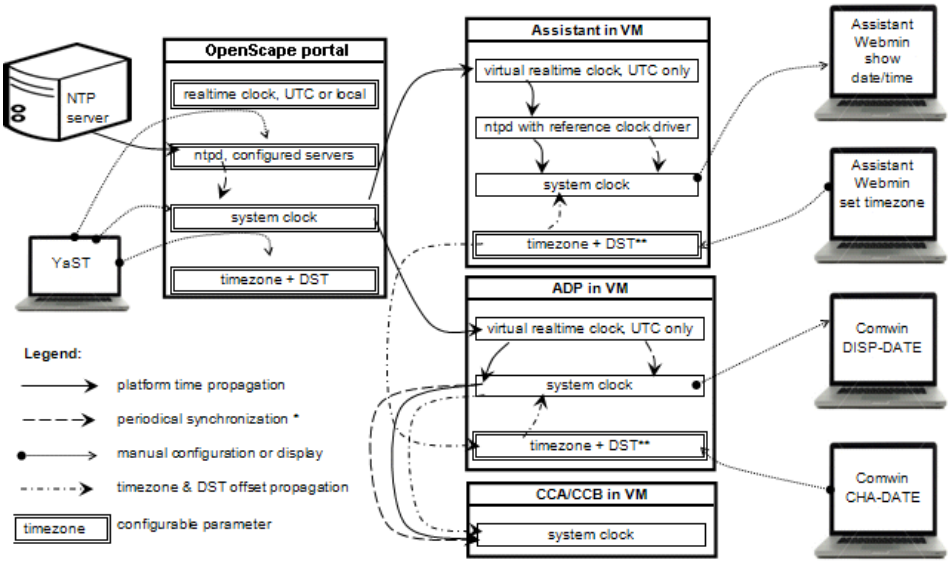
The following operations for date and time configuration for the Manager are possible:

- Selecting the Clock Source (internal or external)
- Date/Time Configuration for the Assistant
- Modifying the Update Interval
- Adding a New Time Server

- Modifying the Time Server Name or IP Address
- Delete a Time Server

10.2 Date/Time Configuration for the Assistant

OpenScape 4000 Date/Time Concept



* The synchronization period for ADP and CCs is 2 minutes.

For the Assistant the ntpd is making fine continuous synchronization. When the step time forward is made on the OpenSape 4000 portal, the Assistant is resynchronized within 3 minutes.

** Daylight savings time offset value

To configure date and time for the Assistant the following steps need to be done:

- Before starting the Assistant, set the current date and time by using the 'YaST' date and time module on the OpenScape 4000 portal.

  You can also set the machine to use the NTP server as a time source. In this case synchronize the time using the `ntpdate` command or wait until the system gets synchronized by the NTP server.

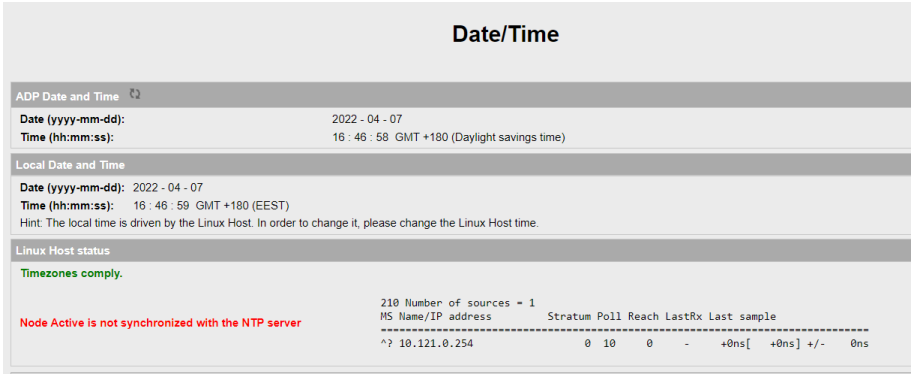
  NOTICE: When the time on the portal is manually shifted *forward*, the Assistant will synchronize in 3 minutes. But before manually shifting time *backward*, make sure that the Virtual Machines are shut down, otherwise the virtual realtime clock on the Assistant gets stuck and the result is unpredictable.

  The timezone configuration is optional as it has no effect on the Assistant's timezone.
- Now start the Assistant.

  The initial date and time is taken from the portal.

- Click the **Date/Time** link in the Assistant's left navigation frame.

  The current date /time setting is displayed in the right frame in 'read-only' mode.



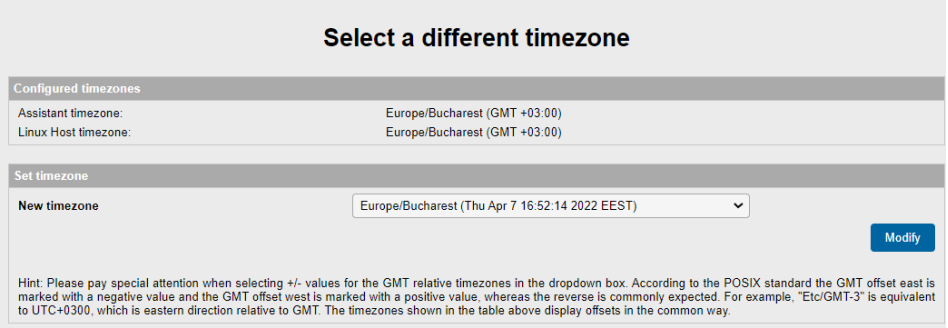
During operation Assistant time is synchronized every few minutes with the portal by ntp deamon with a special reference clock driver. It needs no configuration.

11 Time Zone

This section describes the configuration of the time zone. The configuration of the time zone for Manager and Assistant is handled differently:

- Time Zone Configuration for Manager
- Time Zone Configuration for Assistant

11.1 Time Zone Configuration for Manager



This section describes the configuration of the time zone for OpenScape 4000 Manager.

- You can **modify** time zone by selecting the appropriate time zone in the **New Timezone** list and clicking the **Modify** button.

  The time zone change will take effect immediately.

NOTICE:

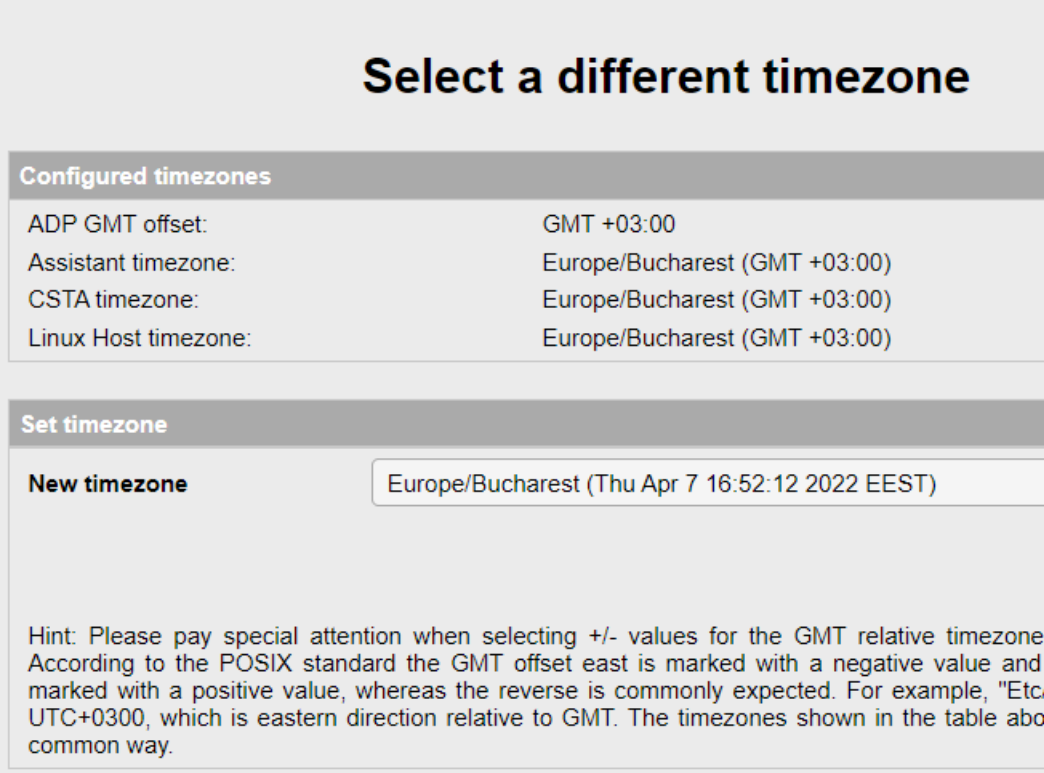
Russia has decided to move to permanent Standard Time starting with 26 October 2014 and onwards. Therefore, two new timezones are created. See http://www.timeanddate.com/news/time/russia-abandons-permanent-summer-time.html for more details.

In order to keep the Manager compliant with these changes, the newest timezone package (minimum version timezone-2014g-0.5.1) with daylight saving time removed must be installed from the SuSE repository. The timezone must be reconfigured in the Webmin Base Administration consequently. When changing the timezone, please pay attention that, according to the POSIX standard, the timezone is marked with a negative value, e.g. "Etc/GMT-3" is equivalent to UTC + 0300.

Related Topic

Time Zone Configuration for Assistant

11.2 Time Zone Configuration for Assistant



This section describes the configuration of the time zone for OpenScape 4000 Assistant. The Assistant is a central point of time zone management for the whole OpenScape 4000 including ADP, CSTA and host platform.

Displayed time zones should match on all these subsystems. If any time zone differs it can be modified here.

- You can **modify** time zone by selecting the appropriate time zone in the **New Timezone** list and clicking the **Modify** button.

When the time zone is modified, the changes are automatically propagated to the host platform, CSTA and ADP.

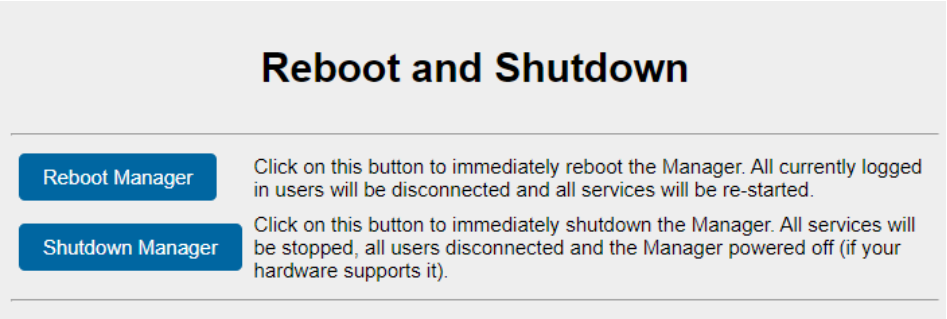
Also the daylight savings time offset, which is controlled by the Assistant, is automatically forwarded to the ADP. The ADP transfers every change of time zone and daylight saving offset immediately to both CCs.

NOTICE: The time zone in the ADP should not be changed manually by the AMO CHA-DATE!

Related Topic

Time Zone Configuration for Manager

12 Reboot / Shutdown System



In order to reboot the system manually, or to shut down the Manager, use the following functions:

- Reboot
- Shutdown (Manager only)

12.1 Reboot

This function can be used for recovery purposes, e.g. if the system is in an abnormal state or for configuration changes to take effect, e.g. when adding a new route.

- You can reboot the system by clicking the **Reboot System** button.

  On the following page you will be asked if you really want to reboot the system.
- Click the button **Reboot System** once again.

  The system is shut down and automatically restarted.

  Please mind that during reboot all currently logged-in users will be disconnected and all services will be re-started.

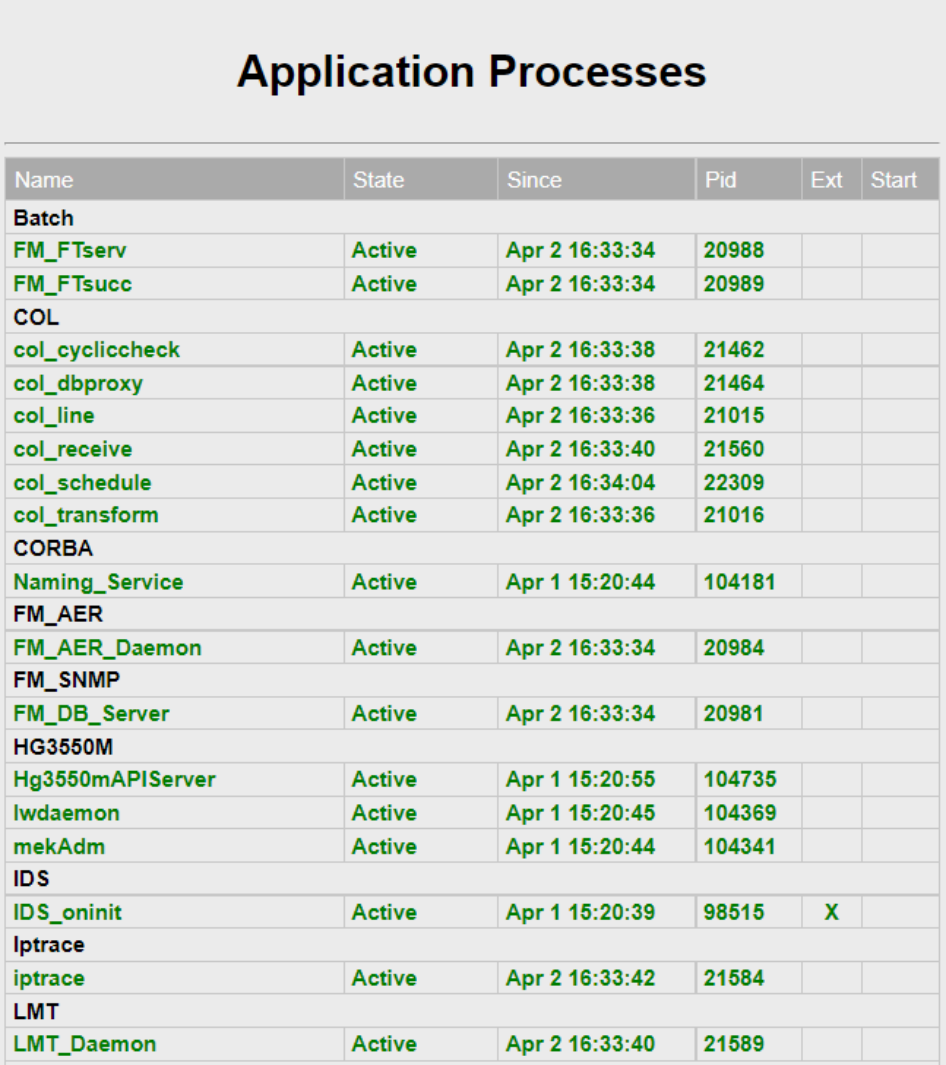
12.2 Shutdown (Manager only)

- You can permanently shut down the Manager using the button **Shutdown System**.
- Confirm if you really want to shut down the system by clicking the button **Shutdown System** on the following page again.

  The system is shut down and powered off (if your hardware supports it).

  The system can only be started again by manual switch on. Please be careful when you are logged on **remotely**, you will not be able to connect again after shutdown. Please mind that all currently logged-in users will be disconnected as a result of the shutdown.

13 Application Processes



Application Processes

Name	State	Since	Pid	Ext	Start
Batch					
FM_FTserv	Active	Apr 2 16:33:34	20988		
FM_FTsucc	Active	Apr 2 16:33:34	20989		
COL					
col_cyclicheck	Active	Apr 2 16:33:38	21462		
col_dbproxy	Active	Apr 2 16:33:38	21464		
col_line	Active	Apr 2 16:33:36	21015		
col_receive	Active	Apr 2 16:33:40	21560		
col_schedule	Active	Apr 2 16:34:04	22309		
col_transform	Active	Apr 2 16:33:36	21016		
CORBA					
Naming_Service	Active	Apr 1 15:20:44	104181		
FM_AER					
FM_AER_Daemon	Active	Apr 2 16:33:34	20984		
FM_SNMP					
FM_DB_Server	Active	Apr 2 16:33:34	20981		
HG3550M					
Hg3550mAPIServer	Active	Apr 1 15:20:55	104735		
lwdaemon	Active	Apr 1 15:20:45	104369		
mekAdm	Active	Apr 1 15:20:44	104341		
IDS					
IDS_oninit	Active	Apr 1 15:20:39	98515	X	
Iptrace					
iptrace	Active	Apr 2 16:33:42	21584		
LMT					
LMT_Daemon	Active	Apr 2 16:33:40	21589		

The Application Processes running in the background provide various OpenScape 4000 Manager/Assistant functions. In the table you can see which processes are running (or not running) and therefore which functionality is available (or not available).

The table of processes displays basic information about all registered processes. Processes are divided into various groups.

Following columns are displayed:

- **Name**

  The name of the process

- **State**

  Following states are possible:

  – **Active**

    The process was started and is still up and running.

  – **Registered**

    The process is registered but not running. It was never started or it was terminated per request by the application. You can start this process by selecting it in the last column and clicking the **Start Selected Process** button.

  – **Inactive**

    The process is not running. It restarted too often (i.e. reached the maximum restart threshold) and was not restarted anymore by the Process Management.

  – **Startup Deferred**

    Process startup is deferred if the process depends on another process which is not running yet.

  – **Startup TimedOut**

    The timeout for process startup was exceeded.

- **Since**

  Creation date of the process

- **Pid**

  Process ID (only for active processes)

- **Ext**

  Process is external, it is started outside the Process Management. External processes cannot be started from here.

- **Start**

  You can start the process which is not running by selecting it and clicking the **Start Selected Process** button.

Index