

A large yellow geometric shape, resembling a stylized triangle or a portion of a circle, is positioned in the top right corner of the page.

Administrator Manual

ECOS SYSTEM MANGEMENT APPLIANCE V6

Manual Version v1.09_EN
November 2017/April 2018

ECOS TECHNOLOGY GMBH
www.ecos.de

© by **ECOS Technology GmbH** 2000 - 2018

Reproduction, distribution and utilization of this document as well as the disclosure of its content are prohibited unless expressly permitted. Offenders will be held liable for the payment of damages. All rights reserved in the event of a patent grant or utility model registration.

Inhaltsverzeichnis

1	ECOS SYSTEM MANAGEMENT APPLIANCE Installation.....	10
2	Layout of the administration interface.....	11
2.1	Login.....	11
2.2	How to customize the sections of the administration interface ..	12
2.3	Information bar	13
2.4	Tree / configuration objects	14
2.4.1	Displaying and hiding subordinate objects.....	14
2.4.2	Context menu.....	15
2.4.3	Moving and copying objects within the tree by drag and drop ...	18
2.4.4	Tree menu bar.....	18
2.4.5	Organizing objects	19
2.5	Menu bar	20
2.5.1	Search	20
2.5.2	Bookmarks.....	20
2.5.3	History.....	21
2.5.4	Previous and next	21
2.5.5	Object add	22
2.6	Configuration objects.....	23
2.6.1	Actions	24
2.6.2	Menu bar of the configuration object.....	25
2.6.3	Selection boxes	28
2.6.4	Tables	29
3	Basic appliance setup.....	41
3.1	Admin user	41
3.2	Network configuration.....	42
3.2.1	Interfaces	42
3.2.2	Defaultgateway and DNS server	43
3.3	Defining network addresses	44
3.3.1	Host/Networks.....	44
3.3.2	Networks	45
3.3.3	Ports.....	45
3.4	Basic services	46
3.4.1	HTTPS administration	46
3.4.2	Radius	46

3.4.3	Software update server	47
3.4.4	Software update	47
3.4.5	Maintenance	47
3.4.6	Time synchronization	48
3.5	Licenses and features	48
4	General configuration objects	50
4.1	Destinations (connection profiles)	50
4.1.1	RDP	51
4.1.2	Citrix	52
4.1.3	VMware	54
4.1.4	Browser	54
4.1.5	Hotspot	55
4.2	Users	56
4.3	Certificates	56
4.3.1	CA certificates	57
4.3.2	X-509 server certificate	59
5	Boot stick configuration and enrolment	61
5.1	Local configuration vs. central management	61
5.2	ECOS SECURE BOOT STICK configuration	61
5.2.1	Services required by the SYSTEM MANAGEMENT APPLIANCE ..	62
5.2.2	ECOS System Connector for SBS	62
5.2.3	How to configure ECOS System Connector with smart card	63
5.3	SBS Personalization	64
5.3.1	Easy Enrollment	65
5.3.2	Easy Enrollment with smart card - SBS [SE] and SBS [SX] only ..	67
5.3.3	Export	68
5.4	SBS VPN	68
5.4.1	Starting the VPN connection	70
5.4.2	IPsec	70
5.5	SBS optional features	70
5.5.1	Boot loader	70
5.5.2	Mass storage	71
5.5.3	Printer	72
5.6	Inheritance	74
5.6.1	Create/configure SBS objects	75
5.7	Information about the management connection	78

5.8	Destinations	78
5.9	Local admin and local user	79
6	Further topics	81
6.1	Log files	81
6.1.1	View/evaluate	81
6.1.2	Configuration	81
6.1.3	Export log information	82
6.2	Updates	82
6.2.1	Local update server vs ECOS update server	82
6.3	How to configure updates servers	83
6.3.1	How to provide images for update servers	84
6.3.2	How to update the appliance	84
6.3.3	Updates for SBS	85
6.4	Directory synchronization	86
6.4.1	Directory service	86
6.4.2	Directory map	88
6.4.3	Directory synchronization	90
6.5	Query	91
6.5.1	Tab 'General'	91
6.5.2	Tab 'Query'	92
6.5.3	Tab 'Fields'	95
6.5.4	Highlights	98
6.6	Bookmarks	98
6.7	Permissions	99
6.7.1	How to create roles	100
6.7.2	How to assign roles to users	100
6.7.3	How to group roles	101
6.7.4	How to assign group permissions	102
6.7.5	Type of permissions	104
6.7.6	Special permission cases	105
7	Technical support	108

1 ECOS SYSTEM MANAGEMENT APPLIANCE Installation

The installation of the appliance requires a virtual machine within a hypervisor. The ECOS appliance is operable under VMware, Hyper-V, Xen Server, KVM as well as various other hypervisors. The virtual machine should meet following minimum requirements:

- 2 CPU cores
- 2 GB RAM
- 100 GB disk space
- 1 Ethernet interface

These values should be increased according to the specific setup.

Begin the installation procedure by starting the virtual machine from the ISO installation image.

In the first step, select the disk on which the appliance should be installed and confirm installation on this disk. After a short copy process, the system is ready to be rebooted. The network data will be requested on the first boot.

This step will require the IP address of the appliance, the default gateway as well as the DNS server. After entering the relevant data, the appliance will boot completely and any further configuration will be made solely in the web-based administration interface.

To fully operate the appliance, upload the licenses via web interface into the configuration object of the appliance.

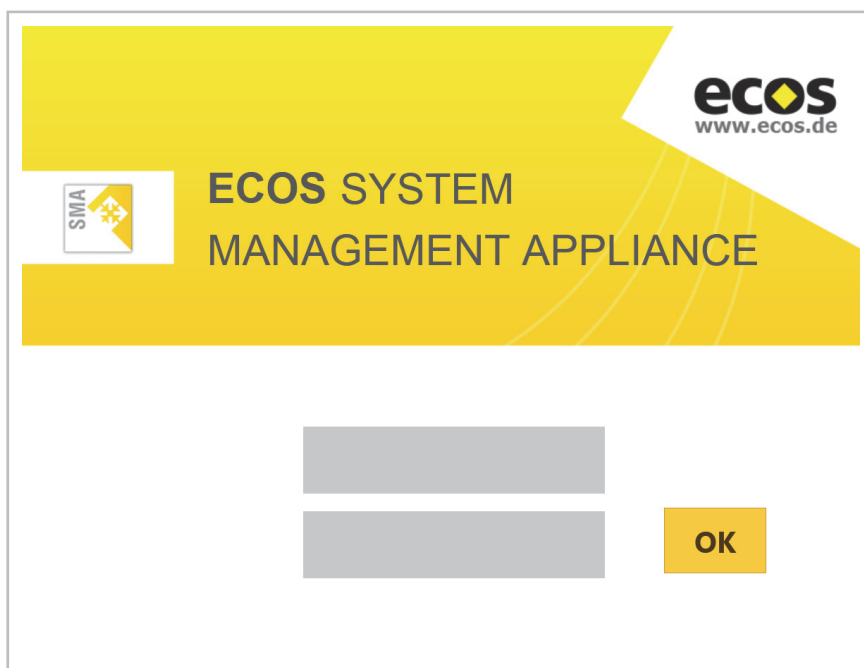
2 Layout of the administration interface

2.1 Login

The administration interface is accessed via web browser and called up through HTTPS on port 543.

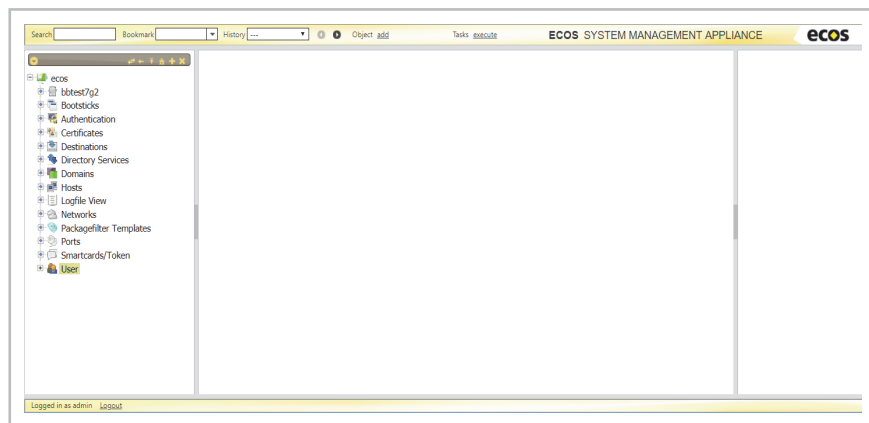
If, for example, the appliance has been installed with the IP address 192.168.1.1, the administration interface will be called up with the URL <https://192.168.1.1:543>.

A login window will appear. In the delivery state, the authentication procedure uses "admin" for user name and "bb5000" as password. The administration interface will be opened after a successful authentication.

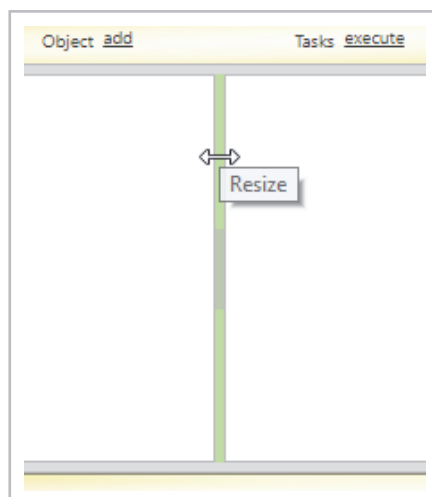
The screenshot shows a web browser window with a yellow header. On the left is the SMA logo (a square with 'SMA' and a stylized sun). On the right is the ecos logo with the website 'www.ecos.de'. The main title 'ECOS SYSTEM MANAGEMENT APPLIANCE' is centered. Below the title are two grey rectangular input fields for username and password. To the right of these fields is a yellow button with the text 'OK'.

2.2 How to customize the sections of the administration interface

The administration interface is composed of three sections with respectively one bar at the top and the bottom. The menu bar is at the top, the tree view on the left, the information bar at the bottom and the section for configuration objects at the center. The different sections are described hereafter.



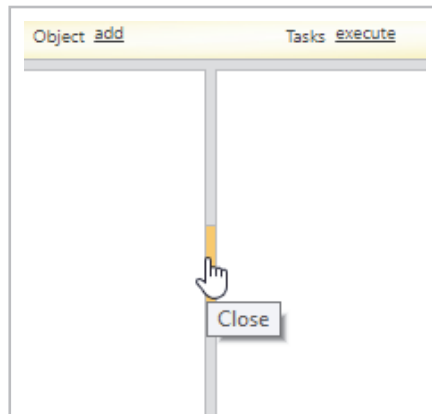
The different sections are marked off by grey separator lines. A double arrow appears when moving the mouse cursor over the separator line.



The size of the sections can be customized by pressing the left mouse button and dragging the mouse cursor to the left or to the right.

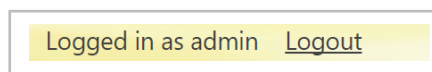
The respective section can be closed by clicking on the darker area at the center of

the separator line. The separator line will then be moved to the edge. A further click on the dark grey area of the separator line opens the section again.



2.3 Information bar

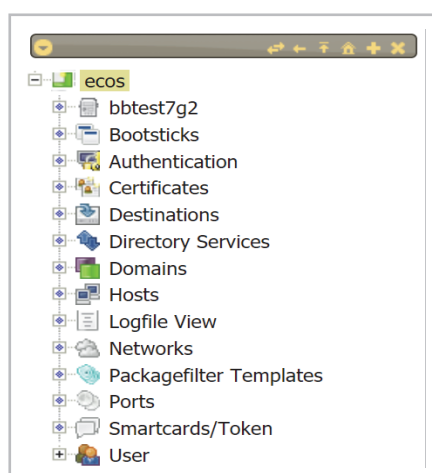
The bar at the bottom edge shows 'Logged in as' to identify the user who is actually logged in. A click on 'Logout' logs the user out and switches back to the login window.



The tree in the left section shows the hierarchical structure of the configuration objects. A click on a configuration object opens its form in the central section of the interface, thus allowing the customization of the object's settings.

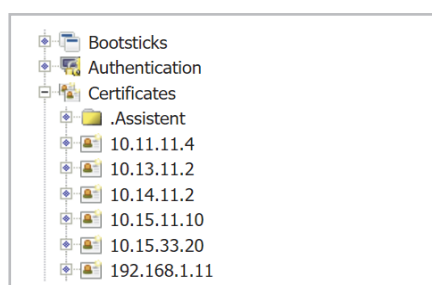
2.4 Tree / configuration objects

Every configuration is performed on configuration objects that contain the actual settings. They are hierarchically displayed on the left side. A minimum number of configuration objects will be created during the installation procedure. These objects can be modified anytime afterwards or deleted if no longer needed. In the same way, new objects can be created to configure advanced features. While some objects can be created anywhere in the tree, most of the objects must be assigned a particular place/container.



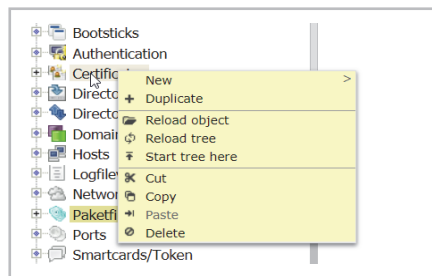
2.4.1 Displaying and hiding subordinate objects.

A click on '+' next to the configuration objects displays subordinate objects. A click on '-' will close the subtrees.



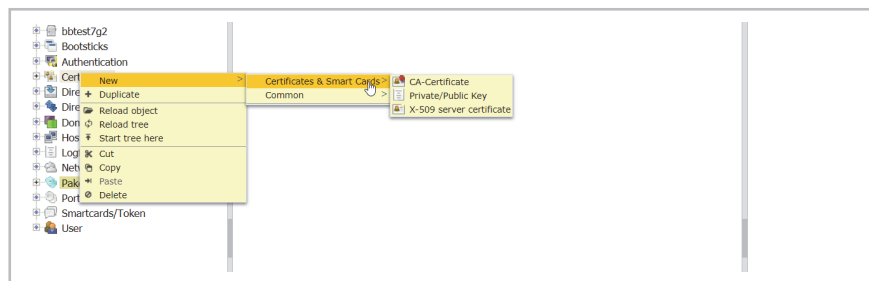
2.4.2 Context menu

A right-click on a configuration object in the tree opens a context menu with following options: 'New', 'Duplicate', 'Reload object', 'Reload tree', 'Start tree here', 'Cut', 'Copy', 'Paste' and 'Delete'.



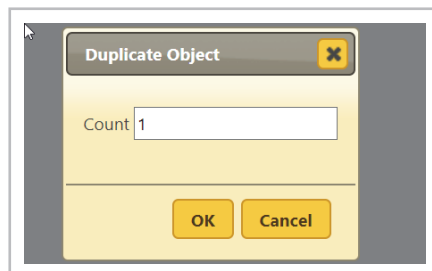
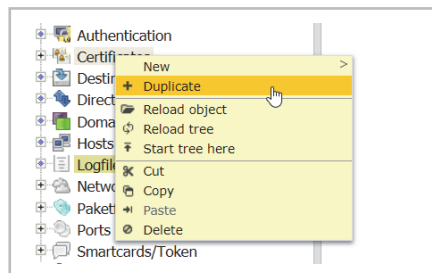
2.4.2.1 New

The menu item 'New' creates subordinate configuration objects for a particular configuration object. The only objects displayed are those actually creatable at this position. Some configuration objects can only be created once. If such an object already exists, it won't be displayed under 'New' anymore. After selection of the object to be created, its form opens in the center section. Enter the required parameters, then save the new object by clicking on the 'Apply' button.



2.4.2.2 Duplicate

A click on 'Duplicate' prompts a window asking how many times the selected configuration object should be duplicated. Hit 'OK' to create the respective number of configuration objects. All duplicated configuration objects possess the same parameters and settings as the template object. The names of the duplicates are automatically numbered consecutively. The button 'Cancel' ends the action without duplicating the selected object.



2.4.2.3 Reload object

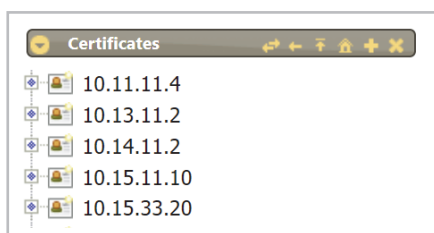
The selected configuration object is reloaded.

2.4.2.4 Reload tree

The subordinate tree is reloaded.

2.4.2.5 Start tree here

This menu item displays only the subtree from the selected configuration object onward instead of the entire tree. A click on the house icon in the tree's menu bar switches the view back to the full tree view.



2.4.2.6 Cut

The selected configuration object is cut and can be inserted elsewhere with the menu item 'Paste'.

2.4.2.7 Copy

The selected configuration object is copied and stored into the cache.

2.4.2.8 Paste

A configuration object previously cut or copied is pasted into the selected position.








2.4.2.9 Delete

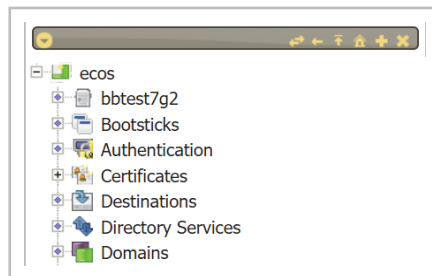
The selected configuration object is deleted.

2.4.3 Moving and copying objects within the tree by drag and drop



Clicking on a configuration object in the tree while holding the left mouse button allows to move the selected configuration object within the tree by drag and drop. The selected object will be placed below the configuration object to which it is dragged. If the selected object can not be positioned under the configuration object to which it has been dragged, it will automatically be placed at the nearest authorized position. A green check mark appears when the mouse cursor points towards a tree position where the selected configuration object can be relocated to. Simultaneously pressing the left mouse button and the control key will copy the selected configuration object instead of moving it.

2.4.4 Tree menu bar

The tree has its own menu bar. A click on the arrow  on the left side of the menu bar will display or hide the tree. Also, the right side of the menu bar shows following options:  'Synchronization with document on/off',  'Synchronize with document now',  'Start tree from current document',  'Display whole tree',  'Display further tree' and  'Close tree'.





2.4.4.1 Synchronization with document on/off

When the feature 'Synchronization with document on/off'  is activated the tree will automatically show the path of the currently opened configuration object. If more than one configuration object is open, the tree will always display the path of the most recently opened or updated object. The icon  indicates that the feature is deactivated.


2.4.4.2 Synchronize with document now

A click on the  icon opens the path of the currently opened configuration object.


2.4.4.3 Start tree from current document

This feature allows to display subtrees separately. A click on the  icon displays only the subtree of the currently opened configuration object from the current document onward. A click on the home icon  allows to go back to the general tree view.

2.4.4.4 Display further tree

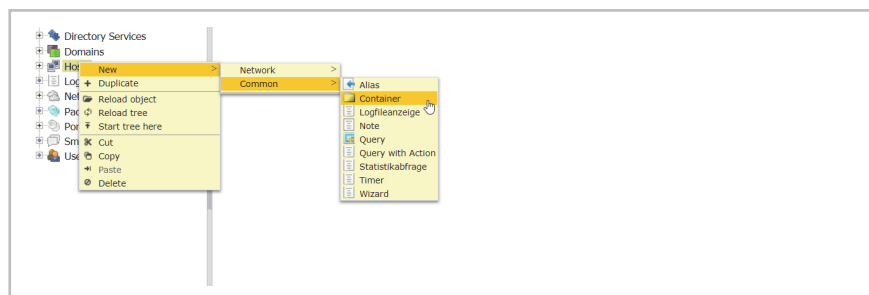
A click on the plus icon  opens another tree and displays it under the already existing tree.

2.4.4.5 Close

Additionally generated trees can be closed by clicking on the cross symbol . If there is only one tree, it can't be closed, only minimized by using the arrow symbol on the left side of the menu bar or by clicking on the dark grey area of the separator line in the left section.

2.4.5 Organizing objects

To improve the general view, configuration objects can always be organized in containers (comparable to folders in the file system). Containers can be created at any tree position and objects can always be moved inside or between the containers. This has no impact on the actual configuration.



Containers can also be used to build groups. Thus, several configuration objects can be created in one container to later allow the selection of the whole container instead of selecting every single configuration object.

2.5 Menu bar

The top menu bar shows the buttons 'Search', 'Bookmarks', 'History', 'Object add' and 'Tasks execute' as well as the arrows for 'previous' and 'next'.



2.5.1 Search

Entering a search term into the box 'Search' will prompt a context menu with configuration objects containing the specified search term in the name. The search box requires at least three letters. Only results containing the requested combination of letters at the beginning of the word will be displayed. It is also possible to combine several search terms by separating them respectively with a blank space. The blank space is equivalent to an AND operation. In this case, only configuration objects containing all search terms will be displayed. Also, the rule for the combination of letters at the beginning of a search term only applies to the first search term. The desired configuration object can be opened in the central section by clicking on its name. Additionally, the configuration object's path will be opened in the tree in the left section.



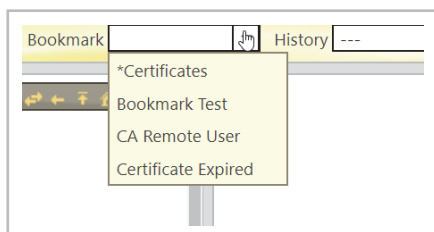
2.5.2 Bookmarks

A click on the arrow on the right side of the box 'Bookmarks' opens a context menu with all bookmarks.

Bookmarks can be set by using the menu bar of the respective configuration object under 'Save view' or by using the 'Action' button below the respective configuration object. See also '2.6.2.1 | Save view' on page 23.

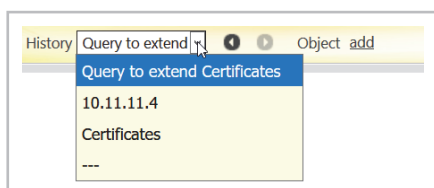
Whole-page bookmarks are prefixed by a *. Bookmark designations without * are related to single objects. The requested configuration object, respectively the whole page with various configuration objects, can be opened with a mouse click on one of the bookmarks.

Instead of opening the context menu by clicking on the arrow on the right side of the box, bookmarks can also be found by name by entering search terms into the box.



2.5.3 History

Clicking on the arrow in the box 'History' opens a pull-down menu showing the most recently opened configuration objects. A click on one of the configuration objects opens it in the central section.



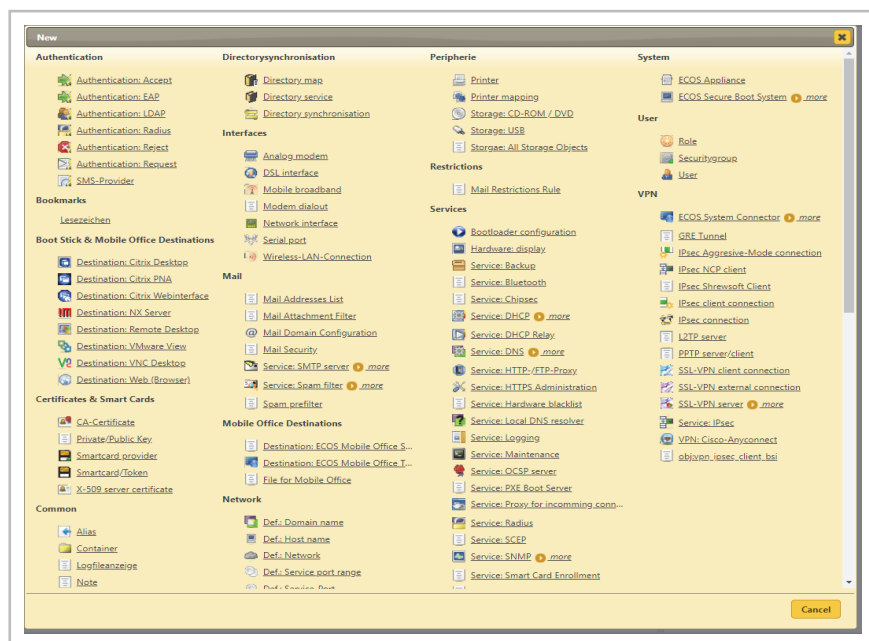
2.5.4 Previous and next

There are two arrows on the right side of the 'History' box. Clicking on the left arrow leads back to the previous configuration object. Clicking on the right arrow opens the next configuration object.

2.5.5 Object add

A click on the button 'Object add' opens a dialogue window listing all the creatable configuration objects. These configuration objects are grouped by category. An arrow showing the mention 'more' next to a configuration object marks subordinate objects that can be displayed with a mouse click on 'more'.

Clicking on the desired configuration object opens its form in which all options can be set. The new object can be stored by clicking on 'Apply'. The configuration object will be automatically created at the first permitted place in the tree.



2.6 Configuration objects

A mouse click on a configuration object in the tree opens it in the central section. The object is composed of a menu bar at the top and the actual form containing the buttons 'Apply' and 'Actions'. Clicking on the button 'Apply' stores the settings that have been entered into the configurations object's form. Closing the configuration object without clicking on 'Apply' prompts an alert message requiring the confirmation or rejection of previous setting changes.

The screenshot displays the 'ECOS Demo CA' configuration window. It features a tabbed interface with 'General', 'History', 'Certificate', and 'Admin' tabs. The 'General' tab is active, showing a form with the following fields and values:

- Name:** ECOS Demo CA
- Description:** (empty)
- Certificate creation:** (dropdown menu)
- Status:** certificate revoked
- Parent-CA:** (dropdown menu)
- Validity:** 1460 days
- Validity of CRL:** 30 days
- URL for CRL distribution point:** (empty)
- URL for authority_info:** (empty)
- Subject:** cn=CA ECOS Demo,ou=SSLVPN Demo,ou=Zertifikate,dc=demo,dc=de
- Issuer:** cn=CA ECOS Demo,ou=SSLVPN Demo,ou=Zertifikate,dc=demo,dc=de
- E-Mail(s):** (empty)
- Keysize:** 2048 Bits
- Signature hash algorithm:** (dropdown menu)
- Fingerprint:** 3D:D8:CC:8E:44:8B:0B:94:C4:E8:CS:8B:EC:A7:1B:42:6F:A5:8A:97
- Valid from:** 04.06.2010, 13:02
- Valid to:** 01.06.2020, 13:02
- Ask for CA password:** Never
- Automatic download of CRL:** (checkbox, unchecked)
- Certificate:** Download Upload Löschen 1 KB
- Private key:** Upload
- Certificate request:** Upload
- CRL:** Download Upload 439 B
- Certificate as PKCS #7:** (empty)
- Certificate as PKCS #12:** (empty)
- Certificate as PEM:** Download 1 KB

At the bottom of the form, there are two buttons: 'Apply' and 'Actions'.

2.6.1 Actions

Clicking on the 'Actions' button opens a context menu that allows to select various actions for the configuration object. The same context menu can be opened by a right-click on the menu bar of the configuration object. The selection of actions coincides with the selection of actions available in the tree's context menu.

2.6.1.1 Clone object

A mouse click on the action 'Clone object' opens a form of the same configuration type and containing the same values as the current configuration object. After entering the relevant object parameters, a new configuration object of the same type can be created and stored by clicking on the 'Apply' button

For further notes on 'Duplicate', 'New', 'Reload object', 'Cut', 'Copy', 'Paste' and 'Delete': See also '2.4.2 | Context menu' on page 13..

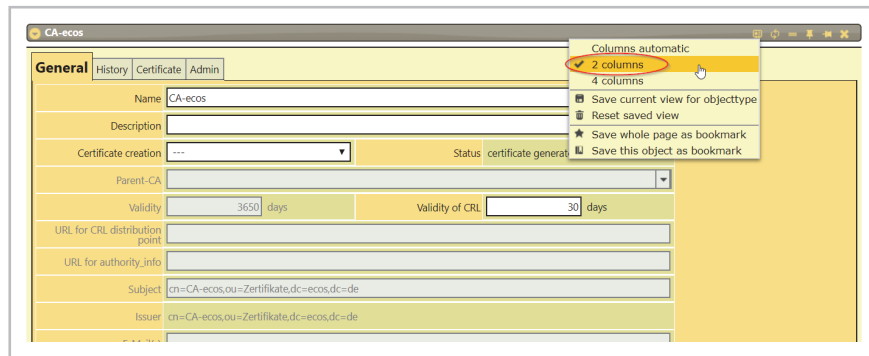
For further notes on 'View', 'Fix in main window', 'Fix in right window' and 'Close': See also '2.6.2.4 | Fix in main window' on page 25.

2.6.2 Menu bar of the configuration object

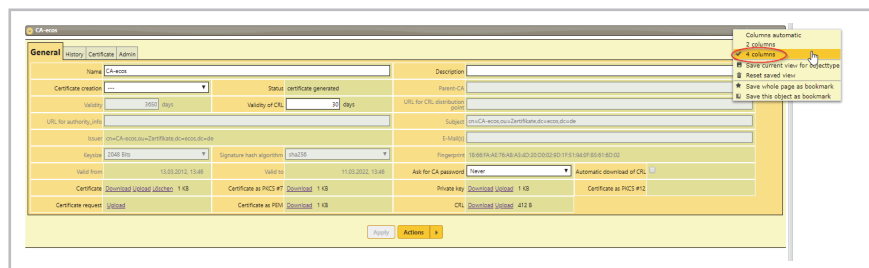
An arrow on the left side of the menu bar allows to pull the form down or up. The right side of the menu bar contains icons for 'Save view', 'Reload', 'Display one below another', 'Fix in main window', 'Fix in right window' and 'Close'.

2.6.2.1 Save view

A click on the 'View' icon opens a context menu with the options 'Columns automatic', '2 columns', '4 columns', 'Save current view for objecttype', 'Reset saved view', 'Save whole page as bookmark' and 'Save this object as bookmark'. The default number of columns is set to '2'. 'Columns automatic' automatically adapts the number of columns that sort the fields to the size of the section.



Selecting '4 columns' displays the form in four columns.



A click on 'Save current view for objecttype' saves the current display settings of the object. All configuration objects of this type will use these settings in the future. In addition to the number of columns, the saved settings also include all settings made in potentially existing tables, such as column width or sorting.

The option 'Reset saved view' deletes the settings from the object type's view. Configuration objects of the same type will subsequently be displayed with the default values.

A click on 'Save whole page as bookmark' opens a new window requiring a name for the bookmark. Confirm by clicking 'OK' to save all configuration objects opened in the current view, tree view included.



A click on 'Save this object as bookmark' saves only the selected configuration object along with all display settings as bookmark. Again, a new window will open and require a name for the bookmark. See also '2.5.2 | Bookmarks' on page 18.

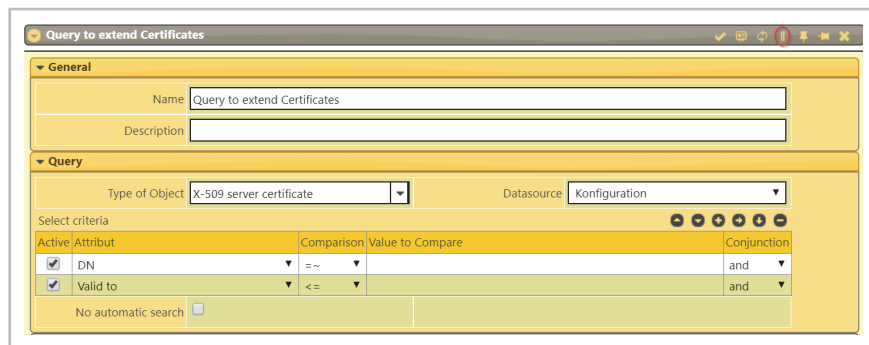
2.6.2.2 Refresh

Clicking on the double-arrow icon reloads the configuration object.




2.6.2.3 Display one below another

A click on the icon with the two horizontal lines  displays the configuration object's tabs one below another. In this view, the tab order can be customized by pressing the left mouse button and moving the tabs. Another click on the  icon switches back to the tab view.




Active	Attribute	Comparison	Value to Compare	Conjunction
<input checked="" type="checkbox"/>	DN	=~		and
<input checked="" type="checkbox"/>	Valid to	<=		and

2.6.2.4 Fix in main window

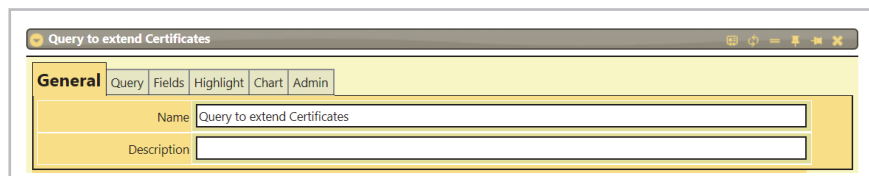
A click on the icon showing the vertical pin  pins the configuration object in the middle section. If another object is opened, the pinned configuration object remains open and will be moved under the newly opened object.

2.6.2.5 Fix in right window

A click on the icon showing the horizontal pin  moves the configuration object to the right section. If more than one object is moved into the right section, the most recent object will always be shown right on top.

2.6.2.6 Show/hide configuration object

A click on the arrow in the configuration object's respective menu bar drops it down or hides it.

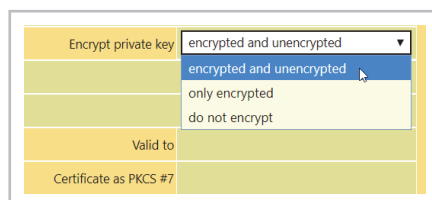


2.6.2.7 Close

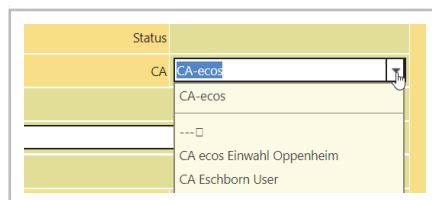
A click on the cross icon  closes the configuration object.

2.6.3 Selection boxes

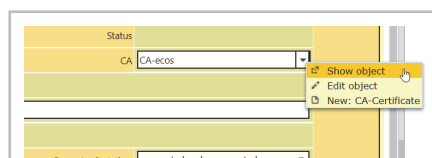
Selection boxes can be related to fixed values, for example key lengths, or to other configuration objects, such as CA. In the latter case, the selection will vary depending on the configuration objects created for this type. Like normal selection boxes, the selection can be displayed by clicking on the arrow. It is also possible to enter a search term into the box. The search uses the same rules as explained in '2.5.1 | Search' on page 18.



Once the selection has been made, a summary of the most important object parameters can be displayed by hovering the mouse cursor over the field. In this view, the parameters can not be changed. To change the settings, the configuration object must be opened.



A right click on the selection opens its menu with the options 'Show object', 'Edit object' and 'New'. These features correspond to the right-click menu explained under '2.6.4.10 | Action column' on page 34.



Additionally, the selection box memorizes the last five selections and shows them as options on top of the list.

Name	Type of Object	Subject	Valid to	Issuer	Modified
ecos					
10.15.33.20	X-509 server certific...				30.08.2016, 04:28
cert ocsp revoked	X-509 server certific...	CN=cert ocsp revoke...			29.08.2017, 08:56
Cert SSL VPN Einwahl...	X-509 server certific...	cn=Cert SSL VPN Ein...		cn=CA ecos Einwahl...	30.08.2016, 04:28
cert test	X-509 server certific...	CN=cert test,OU=zer...			27.09.2016, 10:39
csr test	X-509 server certific...				30.08.2016, 04:28
SSL VPN Demo Client	X-509 server certific...	cn=SSLVPN Demo Cli...		cn=CA ECOS Demo,o...	30.08.2016, 04:28
SSL VPN Demo Server	X-509 server certific...	cn=SSLVPN Demo Co...		cn=CA ECOS Demo,o...	30.08.2016, 08:48

2.6.4 Tables

Many superordinate objects contain a summary table of their subordinate objects. Also, some tables are query results (See also '6.5 | Query' on page 89.).

2.6.4.1 Customizing tables


A double arrow appears in the table header when hovering the mouse pointer over the separator lines of the different columns. The column width can be customized by holding the mouse button and dragging the pointer. A click on a field in the table header while holding the mouse button allows to drag and move the whole column into another position inside the table. Thus, the column order is easily adaptable.

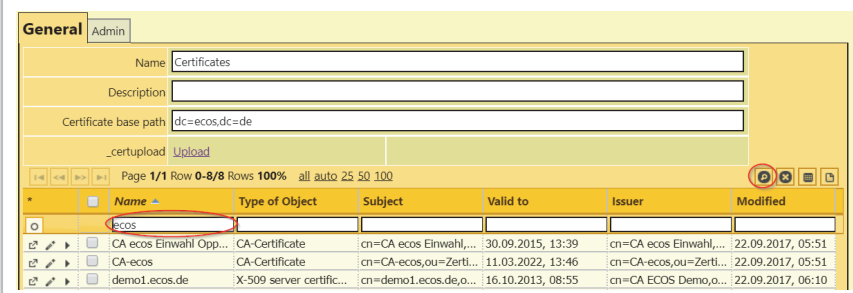
2.6.4.2 Table menu bars

On the right, above the table figure, are five icons with the following features: 'Show filter', 'Remove filter', 'File export' and 'Add object'.

Name	Type of Object	Subject	Valid to	Issuer	Modified
ecos					
10.15.33.20	X-509 server certific...				22.09.2017, 06:10
Cert SSL VPN Einwahl...	X-509 server certific...	cn=Cert SSL VPN Ein...		cn=CA ecos Einwahl...	22.09.2017, 06:10

2.6.4.3 How to use filters in tables

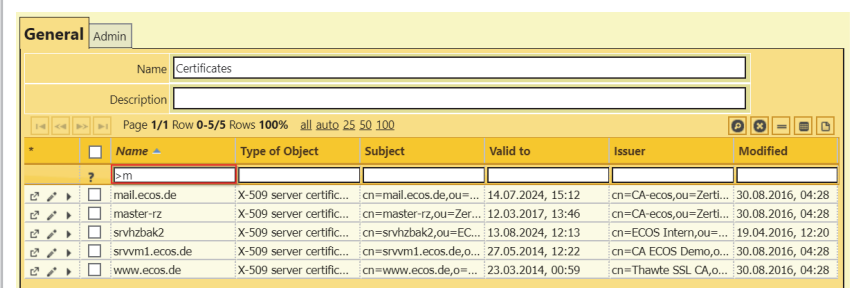
A click on the  icon prompts search boxes above the columns of the table. Entering a search term in one of the search fields restricts the view inside the table to objects which names contain the search term.



The screenshot shows the 'General' tab of the administration interface. The 'Name' field is set to 'Certificates'. The 'Certificate base path' is 'dc=ecos,dc=de'. The table below shows a list of certificates. The 'Name' column is filtered with the term 'ecos'.

Name	Type of Object	Subject	Valid to	Issuer	Modified
ecos	CA-Certificate	cn=CA ecos Einwahl...	30.09.2015, 13:39	cn=CA ecos Einwahl...	22.09.2017, 05:51
CA ecos Einwahl Opp...	CA-Certificate	cn=CA ecos,ou=Zerti...	11.03.2022, 13:46	cn=CA ecos,ou=Zerti...	22.09.2017, 05:51
demo1.ecos.de	X-509 server certific...	cn=demo1.ecos.de,o=...	16.10.2013, 08:55	cn=CA ECOS Demo,o=...	22.09.2017, 06:10

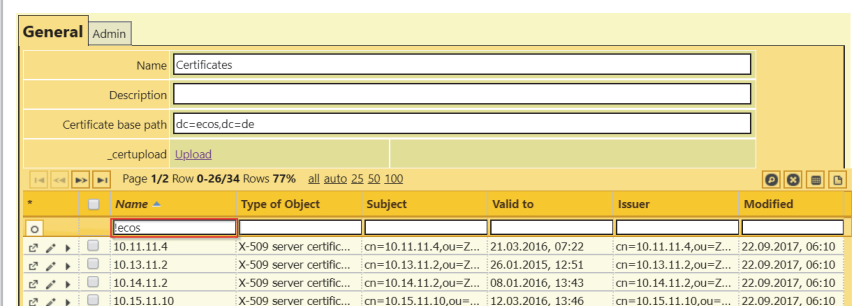
< and > restricts the view to all objects with a value greater or lesser than the reference value in the respective field.



The screenshot shows the 'General' tab of the administration interface. The 'Name' field is set to 'Certificates'. The 'Certificate base path' is 'dc=ecos,dc=de'. The table below shows a list of certificates. The 'Name' column is filtered with the term '>m'.

Name	Type of Object	Subject	Valid to	Issuer	Modified
mail.ecos.de	X-509 server certific...	cn=mail.ecos.de,ou=...	14.07.2024, 15:12	cn=CA ecos,ou=Zerti...	30.08.2016, 04:28
master-rz	X-509 server certific...	cn=master-rz,ou=Zer...	12.03.2017, 13:46	cn=CA ecos,ou=Zerti...	30.08.2016, 04:28
srvhzbak2	X-509 server certific...	cn=srvhzbak2,ou=EC...	13.08.2024, 12:13	cn=ECOS Intern,ou=...	19.04.2016, 12:20
srvvm1.ecos.de	X-509 server certific...	cn=srvvm1.ecos.de,o=...	27.05.2014, 12:22	cn=CA ECOS Demo,o=...	30.08.2016, 04:28
www.ecos.de	X-509 server certific...	cn=www.ecos.de,o=...	23.03.2014, 00:59	cn=Thawte SSL CA,o=...	30.08.2016, 04:28

Preceding the search term with an exclamation mark (!) restricts the view to all configuration objects that don't contain the search term in the respective field.



The screenshot shows the 'General' tab of the administration interface. The 'Name' field is set to 'Certificates'. The 'Certificate base path' is 'dc=ecos,dc=de'. The table below shows a list of certificates. The 'Name' column is filtered with the term '!ecos'.

Name	Type of Object	Subject	Valid to	Issuer	Modified
10.11.11.4	X-509 server certific...	cn=10.11.11.4,ou=Z...	21.03.2016, 07:22	cn=10.11.11.4,ou=Z...	22.09.2017, 06:10
10.13.11.2	X-509 server certific...	cn=10.13.11.2,ou=Z...	26.01.2015, 12:51	cn=10.13.11.2,ou=Z...	22.09.2017, 06:10
10.14.11.2	X-509 server certific...	cn=10.14.11.2,ou=Z...	08.01.2016, 13:43	cn=10.14.11.2,ou=Z...	22.09.2017, 06:10
10.15.11.10	X-509 server certific...	cn=10.15.11.10,ou=...	12.03.2016, 13:46	cn=10.15.11.10,ou=...	22.09.2017, 06:10

Entering * into a search field lists all objects with any details in the respective field.
Entering a - lists all objects with a respective empty field.

The screenshot shows the 'General' tab of the administration interface. The 'Name' field contains the search term '*'. Below the search fields, a table lists the results:

Name	Type of Object	Subject	Valid to	Issuer	Modified
10.15.33.20	X-509 server certifi...				22.09.2017, 06:10
Cert SSL VPN Einwahl...	X-509 server certifi...	cn=Cert SSL VPN Ein...		cn=CA ecos Einwahl,...	22.09.2017, 06:10
cert test	X-509 server certifi...	CN=cert test,OU=zer...			22.09.2017, 06:32
csr test	X-509 server certifi...				22.09.2017, 06:10
SSL VPN Demo Client	X-509 server certifi...	cn=SSLVPN Demo Cli...		cn=CA ECOS Demo,o...	22.09.2017, 06:10

The search fields use regular terms and therefore allow a variety of search terms. For example, 'a|b' allows to search objects containing the value 'a' or 'b' in the corresponding field.

The screenshot shows the 'General' tab of the administration interface. The 'Name' field contains the search term 'a|b'. Below the search fields, a table lists the results:


Name	Type of Object	Subject	Valid to	Issuer	Modified
alecos					
ECOS Demo CA	CA-Certificate				10.09.2017, 16:36

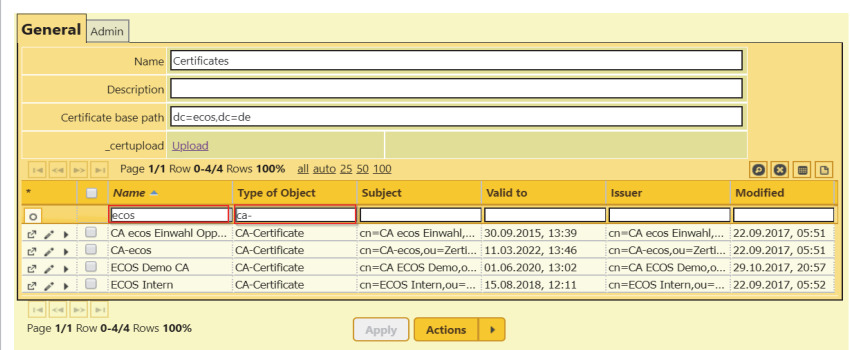
Another helpful input is 'a.*b' to list all objects containing the value 'a' followed by the value 'b' in the respective field, regardless of the possible value range between 'a' and 'b'.

The screenshot shows the 'General' tab of the administration interface. The 'Name' field contains the search term 'a.*b'. Below the search fields, a table lists the results:

Name	Type of Object	Subject	Valid to	Issuer	Modified
ca* ecos					
CA ecos Einwahl Opp...	CA-Certificate	cn=CA ecos Einwahl,...	30.09.2015, 13:39	cn=CA ecos Einwahl,...	22.09.2017, 05:51


There is no case sensitivity.

To specify the search, search terms can be used in several search fields at once. A click on the icon  'Remove filter' resets all filters and all configuration objects will be shown again in the table. Another click on the icon 'Show filter' hides the search fields.




Name	Type of Object	Subject	Valid to	Issuer	Modified
CA-ecos	CA-Certificate	cn=CA ecos Einwahl,...	30.09.2015, 13:39	cn=CA ecos Einwahl,...	22.09.2017, 05:51
CA-ecos	CA-Certificate	cn=CA-ecos,ou=Zerti...	11.03.2022, 13:46	cn=CA-ecos,ou=Zerti...	22.09.2017, 05:51
ECOS Demo CA	CA-Certificate	cn=CA ECOS Demo,o...	01.06.2020, 13:02	cn=CA ECOS Demo,o...	29.10.2017, 20:57
ECOS Intern	CA-Certificate	cn=ECOS Intern,ou=...	15.08.2018, 12:11	cn=ECOS Intern,ou=...	22.09.2017, 05:52

2.6.4.4 File export

A click on the  icon opens a selection menu offering to choose the file types .xlsx or .csv. After selecting the file type, the table will be exported respectively as an excel or comma-separated file and made available for download.

2.6.4.5 Add object

A click on the  icon prompts a pull-down menu listing all configuration objects that are creatable below the object. Selecting the configuration object to be created opens the corresponding form in a new window. After having entered the desired properties, create the object by clicking the 'OK' button.

2.6.4.6 How to sort tables

A click on the title in the table header sorts the table entries accordingly. An arrow next to the title indicates the criterion according to which the table is presently sorted and whether the sorting is ascending (arrow up) or descending (arrow down). A right-click on a field in the table header prompts a context menu containing the features 'Sort ascending and descending' as well as 'Grouping', 'Add Grouping', 'Remove Grouping' and 'Remove Grouping'.

The screenshot shows the 'General' tab of the administration interface. The 'Certificates' section is active. Below the form fields, there is a table with the following columns: Name, Type of Object, Subject, Valid to, and Modified. A context menu is open over the 'Type of Object' header, showing options: Sort ^, Sort v, Grouping, Add Grouping, Remove Grouping, and Grouping. The table contains five rows of certificate data.

Name	Type of Object	Subject	Valid to	Modified
10.11.11.4	X-509 server certific...	cn=10.11.11.4,ou=Z...	21.03.2016	22.09.2017, 06:10
10.13.11.2	X-509 server certific...	cn=10.13.11.2,ou=Z...	26.01.2016	22.09.2017, 06:10
10.14.11.2	X-509 server certific...	cn=10.14.11.2,ou=Z...	08.01.2016	22.09.2017, 06:10
10.15.11.10	X-509 server certific...	cn=10.15.11.10,ou=...	12.03.2016	22.09.2017, 06:10
10.15.33.20	X-509 server certific...			22.09.2017, 06:10

The screenshot shows the same 'Certificates' section. The 'Type of Object' header is now selected, and the table is sorted by this criterion. The table contains five rows of certificate data.

Name	Type of Object	Subject	Valid to	Issuer	Modified
10.14.11.2	X-509 server certific...	cn=10.14.11.2,ou=Z...	08.01.2016, 13:43	cn=10.14.11.2,ou=Z...	22.09.2017, 06:10
SSL VPN Demo Server	X-509 server certific...	cn=SSLVPN Demo Se...		cn=CA ECOS Demo,p...	22.09.2017, 06:10
10.11.11.4	X-509 server certific...	cn=10.11.11.4,ou=Z...	21.03.2016, 07:22	cn=10.11.11.4,ou=Z...	22.09.2017, 06:10
master-rz	X-509 server certific...	cn=master-rz,ou=Zer...	12.03.2017, 13:46	cn=CA-ecos,ou=Zerti...	22.09.2017, 06:10
dnh-fw-2	X-509 server certific...	cn=dnh-fw-2,ou=Zer...	21.03.2017, 07:22	cn=CA-ecos,ou=Zerti...	22.09.2017, 06:10

2.6.4.7 How to group table entries

This feature sorts the table entries according to the selected criterion and groups them below the correspondent title. A click on the arrow displays or hides groups. The number in brackets behind the title shows the number of objects in a group.

The screenshot shows the 'Certificates' administration page. The table has columns: Name, Type of Object, Subject, Valid to, Issuer, and Modified. A context menu is open over the table, showing options: Sort ^, Sort v, Grouping (selected), Add Grouping, Remove Grouping, and Grouping. The table is currently grouped by 'Type of Object: CA-Certificate (11)'.

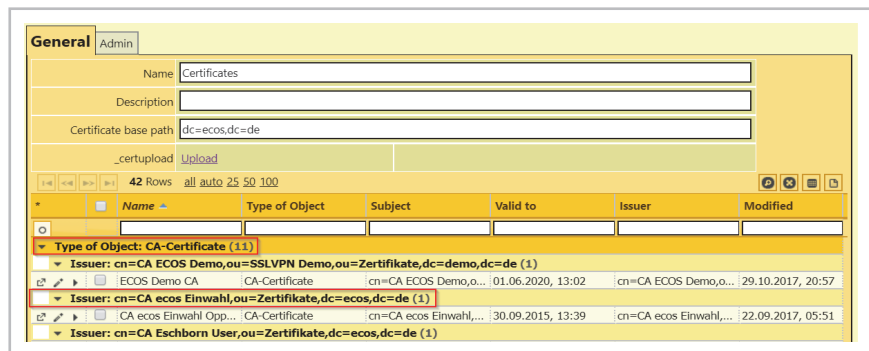
Name	Type of Object	Subject	Valid to	Issuer	Modified
Type of Object: CA-Certificate (11)					
CA ecos Einwahl Opp...	CA-Certificate	cn=CA ecos Einw...		cn=CA ecos Einwahl,...	22.09.2017, 05:51
CA Eschborn User	CA-Certificate	cn=CA Eschborn I...		cn=CA Eschborn User,...	22.09.2017, 05:51
CA Remote User	CA-Certificate	cn=CA Remote U...		cn=CA Remote User,...	22.09.2017, 05:51
ca test	CA-Certificate	CN=ca test,OU=zertif...	22.09.2018, 06:32	CN=ca test,OU=zertif...	22.09.2017, 06:32
CA-ecos	CA-Certificate	cn=CA-ecos,ou=Zerti...	11.03.2022, 13:46	cn=CA-ecos,ou=Zerti...	22.09.2017, 05:51

The screenshot shows the 'Certificates' administration page with the table grouped by 'Subject: (3)'. The table entries are sorted by subject, showing three distinct groups of certificates.

Name	Type of Object	Subject	Valid to	Issuer	Modified
Subject: (3)					
10.15.33.20	X-509 server certific...				22.09.2017, 06:10
csr test	X-509 server certific...				22.09.2017, 06:10
Testzertifikat	X-509 server certific...				23.02.2018, 14:26
Subject: cn=10.11.11.4,ou=Zertifikate,dc=ecos,dc=de (1)					
10.11.11.4	X-509 server certific...	cn=10.11.11.4,ou=Z...	21.03.2016, 07:22	cn=10.11.11.4,ou=Z...	22.09.2017, 06:10

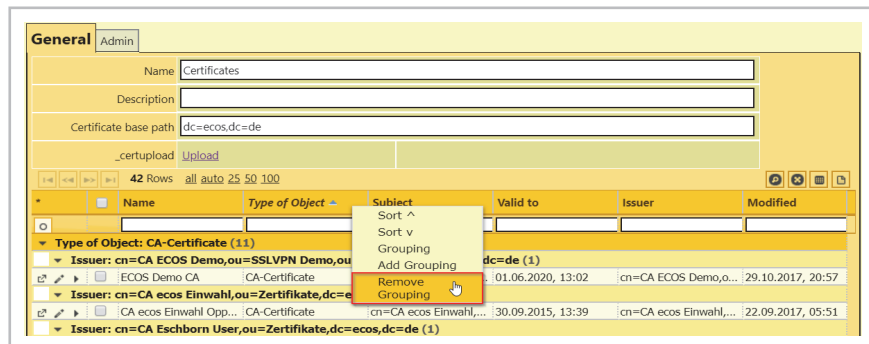
2.6.4.8 Add grouping

This feature allows to sort and club together already existing groups (such as object type) in subgroups by using further criteria (such as issuer).






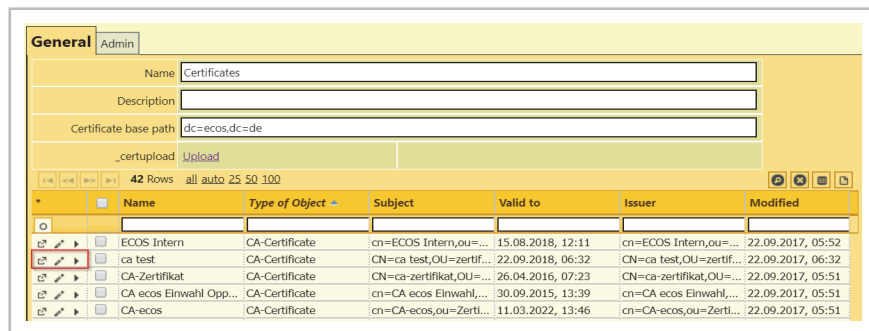
2.6.4.9 Remove grouping

Selecting 'Remove Grouping' dissolves all existing groupings

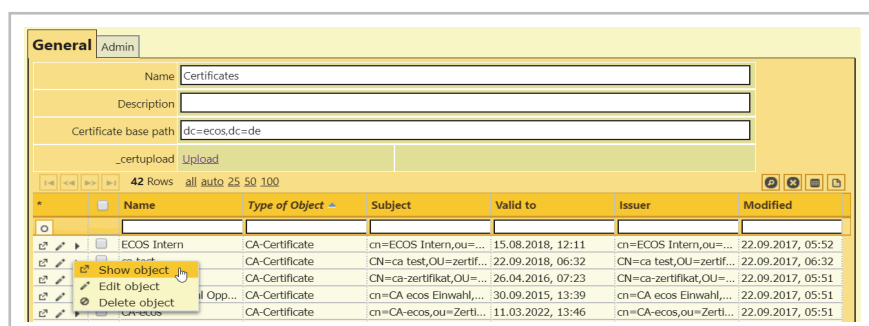


2.6.4.10 Action column

Icons for  'Show object',  'Edit object' and  'Display object' figure on the left of each object inside the table.




Alternatively, a right-click on the button prompts a pull-down menu with the options 'Show object', 'Edit object' and 'Delete object'.

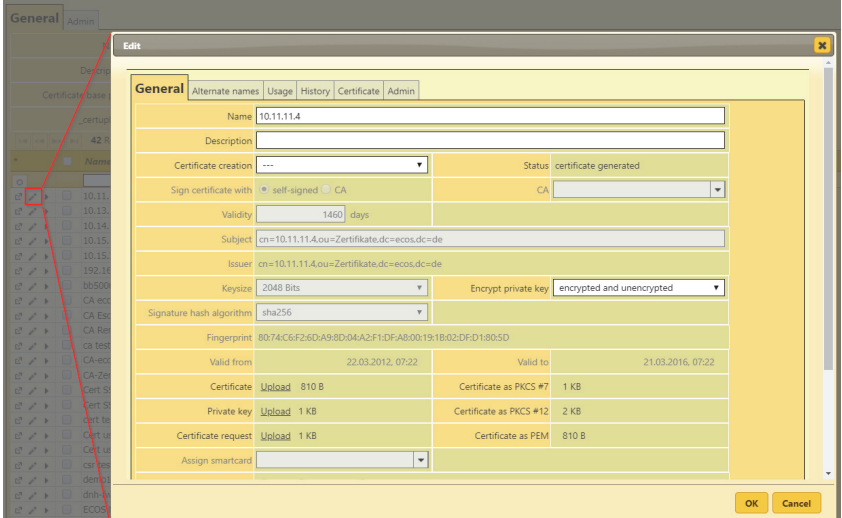


2.6.4.11 Show object

A click on the icon  opens the correspondent configuration object in the central section. Alternatively, a click on a table field with the middle mouse button opens the configuration object too.

2.6.4.12 Edit object

A click on the  icon opens the configuration object's form in a new window. Alternatively, the form can be opened by a double-click on a table field of the configuration object. The form allows to customize the settings of the configuration object. Save the changes by clicking 'OK'.



The screenshot shows the 'Edit' dialog box for a configuration object. The dialog has tabs: General, Alternate names, Usage, History, Certificate, Admin. The 'General' tab is active. It contains the following fields and options:

- Name: 10.11.11.4
- Description:
- Certificate creation: ---
- Status: certificate generated
- Sign certificate with: self-signed CA
- Validity: 1460 days
- Subject: cn=10.11.11.4,ou=Zertifikate,dc=ecos,dc=de
- Issuer: cn=10.11.11.4,ou=Zertifikate,dc=ecos,dc=de
- Key size: 2048 Bits
- Encrypt private key: encrypted and unencrypted
- Signature hash algorithm: sha256
- Fingerprint: 80:74:C6:F2:6D:A9:8D:04:A2:F1:DF:A8:00:19:1B:02:DF:D1:80:5D
- Valid from: 22.03.2012, 07:22
- Valid to: 21.03.2016, 07:22
- Certificate: Upload 810 B
- Certificate as PKCS #7: 1 KB
- Private key: Upload 1 KB
- Certificate as PKCS #12: 2 KB
- Certificate request: Upload 1 KB
- Certificate as PEM: 810 B
- Assign smartcard:

Buttons: OK, Cancel

2.6.4.13 Show object

A click on the ► icon displays a summary of the most important parameters of the configuration object. Another click on the ▼ icon hides them.

General Admin

Name: Certificates

Description:

Certificate base path: dc=ecos,dc=de

_certupload: Upload

43 Rows all auto 25 50 100

Name	Type of Object	Subject	Valid to	Issuer	Modified
10.11.11.4	X-509 server certific...	cn=10.11.11.4,ou=Z...	21.03.2016, 07:22	cn=10.11.11.4,ou=Z...	22.09.2017, 06:10
10.13.11.2	X-509 server certific...	cn=10.13.11.2,ou=Z...	26.01.2015, 12:51	cn=10.13.11.2,ou=Z...	22.09.2017, 06:10
10.14.11.2	X-509 server certific...	cn=10.14.11.2,ou=Z...	08.01.2016, 13:43	cn=10.14.11.2,ou=Z...	22.09.2017, 06:10
10.15.11.10	X-509 server certific...	cn=10.15.11.10,ou=...	12.03.2016, 13:46	cn=10.15.11.10,ou=...	22.09.2017, 06:10

Object Details:

Name: 10.15.11.10

Status: certificate generated

Validity: 1460 days

Subject: cn=10.15.11.10,ou=Zertifikate,dc=ecos,dc=de

Issuer: cn=10.15.11.10,ou=Zertifikate,dc=ecos,dc=de

Keysize: 2048 Bits

Signature hash algorithm: sha256

Fingerprint: 48:1D:71:13:31:C8:90:49:FA:9B:81:48:69:DC:90:1C:BC:B2:FB:C3

Valid from: 13.03.2012, 13:46

Valid to: 12.03.2016, 13:46

2.6.4.14 Delete object

The selected object is deleted. If several objects have been selected, an alert message appears requiring to confirm the deletion of the selected objects.

General Admin

Name: Certificates

Description:

Certificate base path: dc=ecos,dc=de

_certupload: Upload

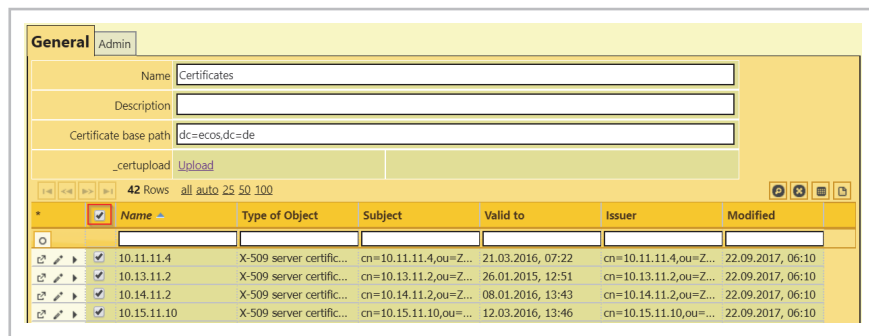
42 Rows all auto 25 50 100

Name	Type of Object	Subject	Valid to	Issuer	Modified
10.11.11.4	X-509 server certific...	cn=10.11.11.4,ou=Z...	21.03.2016, 07:22	cn=10.11.11.4,ou=Z...	22.09.2017, 06:10
10.13.11.2	X-509 server certific...	cn=10.13.11.2,ou=Z...	26.01.2015, 12:51	cn=10.13.11.2,ou=Z...	22.09.2017, 06:10
10.14.11.2	X-509 server certific...	cn=10.14.11.2,ou=Z...	08.01.2016, 13:43	cn=10.14.11.2,ou=Z...	22.09.2017, 06:10
10.15.11.10	X-509 server certific...	cn=10.15.11.10,ou=...	12.03.2016, 13:46	cn=10.15.11.10,ou=...	22.09.2017, 06:10
192.168.1.11	X-509 server certific...	cn=192.168.1.11,ou=...	17.12.2017, 11:49	cn=192.168.1.11,ou=...	22.09.2017, 06:10

Buttons: Show object, Edit object, Delete object

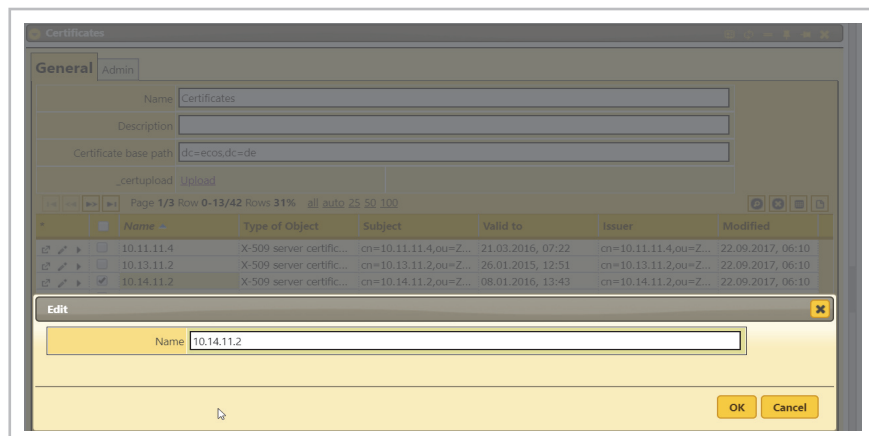
2.6.4.15 Selecting objects in tables

A click on the selection box in the table header selects all configuration objects in the table. A click on the box next to a configuration object selects it. Thus, it is possible to select several objects inside the table. Alternatively, click on a random field inside the table to select one object and hold to select more objects.



2.6.4.16 Edit table fields

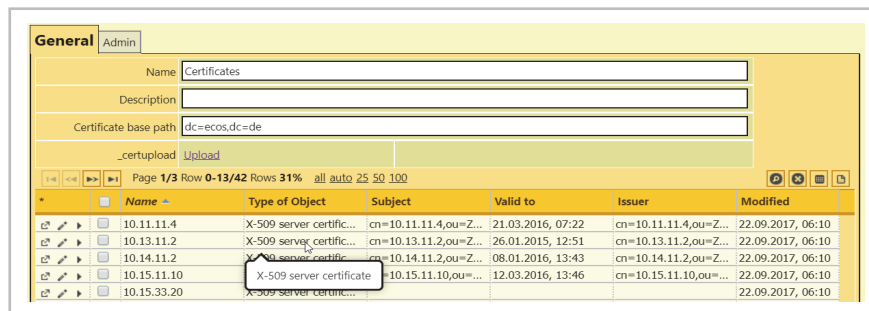
A right-click on a table field shows the option 'Edit'. Selecting this option opens a new window in which the field content, whenever editable, can be modified. A click on 'OK' stores the changes. If more than one object has been selected, the content of all fields will change accordingly.



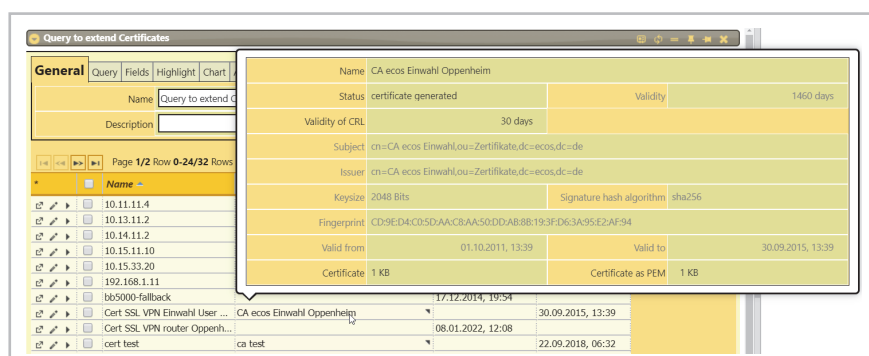
A black triangle in the upper right corner of a table field means that the field's content refers to another configuration object. The context menu of these fields additionally contains the options 'Show object' and 'Edit object'.

2.6.4.17 Popups

When a column isn't broad enough to show the whole text, move the mouse pointer over the table field. This will prompt a popup showing the full text.



If a table field entry is related to another configuration object, moving the mouse pointer over the field while holding the shift key opens a summary of the object's main parameters.



3 Basic appliance setup

3.1 Admin user

To administrate ECOS SYSTEM MANAGEMENT APPLIANCE, every admin user has to log in. See also '2 | Layout of the administration interface' on page 9.

It is possible to create one or more admin users. In the delivery state, the user "admin" is predefined and endowed with administrator privileges. Administrators have an unrestricted access to all configuration objects und features.

Administrator privileges can be assigned in the tab 'General' by ticking the checkbox 'Admin access'. The user in question has then access to all management features.

The screenshot displays the 'General' tab of the user configuration interface. The tab is highlighted in yellow. Below the tab, there are several sub-tabs: 'Login', 'Destinations', 'Personal data', 'Certificate', and 'Admin'. The 'Login' sub-tab is active. The form contains the following fields and controls:

- Name:** Text input field containing 'admin'.
- Login:** Text input field containing 'admin'.
- Description:** Text input field.
- Surname:** Text input field.
- Department:** Text input field.
- Password:** Password input field with masked characters (dots).
- Password re-enter:** Password input field with masked characters (dots).
- Admin access:** Checkable checkbox, currently checked.
- Do not hash password:** Checkable checkbox, currently unchecked.
- Access to admin interface:** Checkable checkbox, currently unchecked.
- Role:** Dropdown menu showing '---'.

At the bottom of the form, there are two buttons: 'Apply' and 'Actions'.

It is also possible to tick the checkbox 'Access to admin interface' to allow the user to access the administration web interface.

General		Spam filter	Mail filter	Mobile Office	Virtual Web	Authentication	Certificates
Login	Destinations	Personal data	Certificate	Admin			
Name	admin		Login	admin			
Description							
Surname			Department				
Password	*****		Password re-enter	*****			
Admin access	<input type="checkbox"/>		Do not hash password	<input type="checkbox"/>			
Access to admin interface	<input checked="" type="checkbox"/>		Role	---			
<div> Apply Actions </div>							

If no further user privileges have been conferred, the field is empty. A user can be endowed with specific privileges by assigning him a role.

See also '4.2 | Users' on page 54. and '6.7.2 | How to assign roles to users' on page 98

3.2 Network configuration

The basic network configuration is made by creating the necessary interfaces in the container 'Interfaces' on one hand, on the other hand by setting the default gateway and the DNS server/s within the system object of the appliance. Furthermore, static routes can be added to the container 'Routes'.

3.2.1 Interfaces

The desired network interfaces can be created in the container 'Interfaces' below the management appliance object. Various objects are available depending on the device type.

In the delivery state, a LAN object already figures in the container 'Interfaces' and will require the configuration of the IP address and the net mask of the desired network. If more than one LAN interface is needed, any desired number of network interfaces can be created and configured.

The screenshot shows the 'General' tab of a configuration interface for a LAN. The tabs at the top are 'General', 'Current Status', and 'Admin'. The form contains the following fields:

- Name:** A text input field containing 'LAN'.
- Description:** An empty text input field.
- Obtain IP address:** Two radio buttons, 'Fixed IP' (selected) and 'from DHCP'.
- IP-Address:** A text input field containing '10.161.200.183'.
- Net mask:** A dropdown menu showing '/24 (255.255.255.0)'.
- Device name:** A dropdown menu showing 'LAN-1'.
- VLAN ID:** An empty text input field.
- Define as main interface:** An unchecked checkbox.
- ARP update:** An unchecked checkbox.

At the bottom of the form are two buttons: 'Apply' and 'Actions' with a right-pointing arrow.

3.2.2 Defaultgateway and DNS server

It is necessary to configure a default gateway and a DNS server in the tab 'Network' of the appliance object. If required, further static routes can be added in the container 'Routes' of the appliance object.

The screenshot shows the 'Network' tab of a configuration interface. The tabs at the top are 'General', 'Network' (active), 'Dependencies', 'Software licenses', 'Actions', 'Info', and 'Admin'. The form contains the following fields:

- DNS Server:** A dropdown menu showing 'Standard Gateway'.
- Low priority for DNS servers:** An unchecked checkbox.
- Gateway:** A dropdown menu showing 'Standard Gateway'.
- PXE Boot Enable:** An unchecked checkbox.
- MAC Address for PXE:** An empty text input field.
- PXE Kernel Parameter:** An empty text input field.

At the bottom of the form are two buttons: 'Apply' and 'Actions' with a right-pointing arrow.

3.3 Defining network addresses

3.3.1 Host/Networks

The configuration object 'Def.: Hostname' defines a name for a computer or an IP address. With this name, the host can be referenced at various places whenever IP addresses are required. The central definition of host addresses allows an easy host management as the actual address has to be entered only once. Whenever the IP address needs to be changed, the change is only performed in the host definition and applies to all places where this host has been referenced.

The type of a host object specifies how the IP address will be determined. Options available are 'dynamic', 'static' or 'manual'.

General		Tools	Admin
Name	h-demo1.ecos.de		
Description			
IP address or hostname	demo1.ecos.de	Priority	500
Type	<input checked="" type="radio"/> dynamic <input type="radio"/> static <input type="radio"/> manual		
IP-Address	176.9.134.61		
<div>Apply Actions</div>			

If a host is of type 'dynamic' and a DNS name is entered, the IP address will be determined from this name and it will continually be checked whether the address changes. This is useful for dynamic DNS names.

When the type 'static' is selected, the DNS name will only be translated into an IP address when it's mentioned. If the IP address of an already specified DNS name is modified, it must be confirmed by clicking again on the 'Apply' button. This type protects against DNS spoofing, as false or malignant DNS entries can't modify the IP address retroactively.

When the type 'manual' is selected, the IP address must be entered manually and will not be determined through DNS. In this case, an entry will be added to the 'hosts'-file to make the name available to all programs/services on the system, even if there is no connection to a DNS or if the host can't be resolved by DNS.

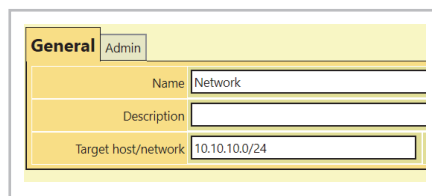
For the types 'dynamic' and 'static', the determined IP address will be displayed in the field 'IP address'. For the type 'manual', the IP address must be entered manually.

The field 'Priority' allows to assign various priorities to hosts that can be used for sorting in lists. An example of application is when a container includes different hosts and is then specified as DNS server. In this case, the priority determines which DNS server will be queried first. Smaller numbers mean higher priority.

3.3.2 Networks

Network addresses are managed by the configuration objects 'Def.: network'. These define names for IP networks. The network can be referenced by its name at various places where network addresses are required. Furthermore, the central definition of network addresses allows easy modifications as the actual address must only be specified once. The network address needs to be modified only in the network definition and the change will directly affect all places where this network has been referenced.

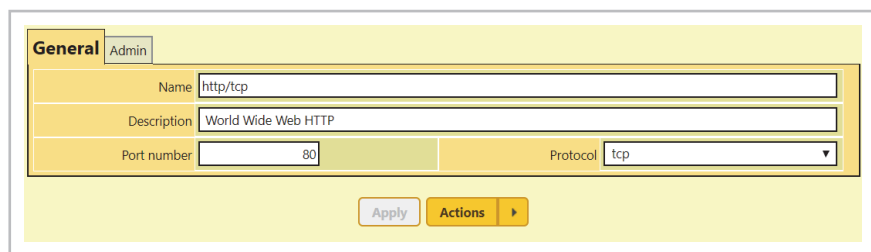
IP address and net mask of the network defined in the name field are specified in the field 'Target host/network' in form of n.n.n.n/m.



General		Admin
Name	Network	
Description		
Target host/network	10.10.10.0/24	

3.3.3 Ports

Ports are managed by the configuration objects 'Def.: Service Port'. Here, a name can be assigned to a specific UDP or TCP port. On other occasions, when a configuration requires a port selection, the corresponding port should be referenced by the assigned port name.



General		Admin
Name	http/tcp	
Description	World Wide Web HTTP	
Port number	80	Protocol: tcp ▼
<div> Apply Actions ▶ </div>		

3.4 Basic services

3.4.1 HTTPS administration

The service 'HTTPS Administration' allows the configuration of the HTTPS server that provides the administration interface.

The server certificate is selected in the field 'HTTPS Server Certificate' through which the ECOS system is authenticated when launching the administration interface. A default certificate is generated during the installation procedure and can be replaced by a certificate customized to the actual environment so the browser trusts the administration interface.

The field 'HTTPS Server Port' allows the configuration of the port specifically used to launch the administration interface. The default port of the appliance is set to 543 to avoid conflicts with other services that might use the normal HTTPS port 443. If not port is set, the default port will be 443.

In the field 'HTTPS server address' allows to set the address under which the administration interface will be available. If the field is left empty (default case) while the appliance has several addresses, it can be reached under each of them.

The type of authentication on the administration interface of the appliance can be set in 'Admin Login'. The default setting is 'Password only'. In this case, the user logs in with his respective static password. See also '3.2 | Network configuration' on page 40.

When selecting the option 'Password and certificate', authentication is only possible if the user additionally holds a valid certificate. This certificate must be issued by the CA specified for certificate login (field 'CA for certificate login'). This certificate can be either a software certificate stored on the user computer or a certificate stored on a smart card or a token.

3.4.2 Radius

The Radius service ensures the authentication of different services. It must be created and started in the appliance object of the container 'Services'.

The Radius service is required for Easy Enrollment per activation code. If, apart from Easy Enrollment, there are no further services to authenticate by the Radius service, no further settings are required.

When Easy Enrollment is performed via smart card, the Radius service is not required.

3.4.3 Software update server

The software update server service is required for both Easy Enrolment and boot stick connections. Besides, it can also distribute software updates to boot sticks or further appliances. See also '6.3 | How to configure updates servers' on page 81.

To connect boot sticks it is only necessary to create and start the software update server serviced.

General		Admin
Name	Software Update Server	Start <input checked="" type="checkbox"/>
Description		
HTTPS server address		HTTPS server port
Default for Updates		

3.4.4 Software update

The software update service is described here: See also '3.4.4 | Software update' on page 45.

3.4.5 Maintenance

The service 'Maintenance' allows to configure maintenance accesses.

The settings for the local maintenance access is configured in the tab 'Local maintenance'. Ticking the checkbox 'Activate password for console' activates the user-defined password for login on the console. Log in with the username 'setup'. If no password has been set, the default password is 'bb5000'. Shell or root access in no way available via console. There is only access to a menu that allows basic maintenance tasks, for example setting the IP address or sending a ping.

```

Current configuration:
  IP Address: 10.161.200.175/24
  Address of the default gateway: <unbekannt>
  Paket filters: set
  URL of the configuration interface: https://10.161.200.175/

Please select
A .. Set IP address           F .. Delete packet filters
G .. Set default gateway      X .. Show iptables
I .. Show interfaces addresses H .. Start SSH
J .. Show interfaces states   D .. Restart DSL
W .. network setup           M .. Show routing table
Z .. Process control          O .. Show detailed routing table
L .. Logfile viewer           E .. Show extended routing table
P .. Execute ping             U .. Show routing policies
T .. Execute traceroute       Y .. system state
M .. Maintenance Mode         U .. ldap cache reset
C .. Restart configuration process R .. Reset to factory defaults
K .. Show networktraffic       O .. Reboot
9 .. Poweroff                 B .. Restore last backup
S .. Run base-setup in text mode Q .. Quit

Please select an action: _

```

Ticking the checkbox in the tab 'Remote maintenance' enables the SSH remote maintenance. The port you wish to react to the SSH service can be specified in the field 'Port'. If the field is left empty, the default SSH port 22 will be used. It is possible to login via 'SSH' as user 'remotesetup' and access the same menu that is used for the direct console login.

This requires a password in the field 'Password remote maintenance'. Additionally, it is possible to enable SSH port forwarding on some ports for the user 'remotesetup'. These can be specified in the field 'Allowed forwarded ports'.

3.4.6 Time synchronization

The service 'Time synchronization' automatically sets the correct local time via NTP protocol. The mention of one or more NTP server is required.

3.5 Licenses and features

The user has access to different features depending on the license that has been purchased. These features are summarized in the appliance object in the tab 'Software licenses'.

If the ECOS update server is used for update management, the latest activated licenses will be automatically distributed by the update server to the management appliance respectively the boot sticks during the update procedure.

For further information about the update management: See also '6.3 | How to configure updates servers' on page 81.

However, the management appliance will only load its own licenses from the update server. If licenses should be distributed to boot sticks, they have to be loaded as zip files (see below).

If a local update server is used for update management, the appliance must be provided with new licenses in the form of zip files. The zip file contains the necessary licenses required by the management appliance and all related boot sticks.

The option 'Load licenses' can be found in the menu bar in the upper section of the screen under 'Tasks execute'. This menu item allows to activate license-based features and load licenses in form of zip files.

A click on 'Load license' opens a new window in which the license file can be selected and loaded by clicking on 'Next'.

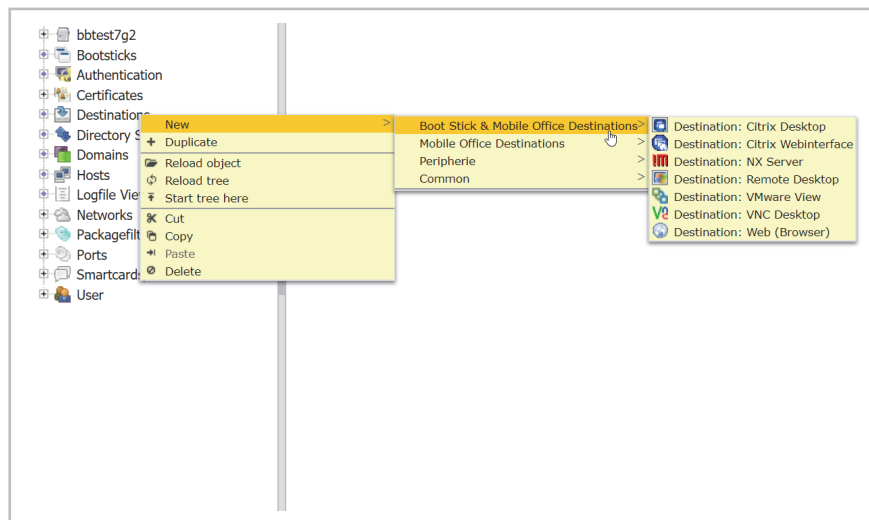
It is also possible to load single licenses for a specific appliance or a specific boot stick in the appliance or boot stick object in the tab 'Software licenses'.

4 General configuration objects

4.1 Destinations (connection profiles)

To allow the remote access to a terminal server or another destination system via boot stick, it is required to create connection profiles or so-called destinations. Destinations are those systems to which the user actually has access. The data required for the connection establishment are to be specified in the corresponding configuration objects.

All destinations have to be created below the configuration object of the type 'Container: Destinations'. 'Destinations' is the default name of the container. The container 'Destinations' includes a summary of all created destinations. Below the container are all existing destination objects. New destination objects can be created and configured here. Supported destination systems are Microsoft Terminal Server, Citrix, VMware Horizon and web servers.



4.1.1 RDP

The Remote Desktop Protocol (RDP) allows to access a terminal server through the ECOS boot stick. For this, create a new configuration object 'Destination: Remote Desktop' below the container 'Destinations'.

Every RDP destination object requires a name under which it will be stored and displayed to the user in the destination's selection window. Optionally, the RDP object can be complemented by a description and an internal description. The description will also be shown to the ECOS SECURE BOOT STICK user.

The screenshot displays the 'General' tab of an RDP configuration window. It features a grid of input fields and checkboxes. Key fields include 'Name', 'Description', 'Internal description', 'Server Address' (with a dropdown), 'Port' (with a dropdown), 'User name', 'Password', 'Domain', 'Screen resolution' (with a dropdown), 'Color depth' (set to 24 Bit), 'Keyboard layout' (set to English (USA)), 'Window title', 'Hide window decoration' (checkbox), 'Compression' (checked), 'Activate cache' (checked), 'Disable encryption' (checkbox), 'Network level authentication' (checkbox), 'Bandwidth' (set to LAN), 'Multimonitor support' (checkbox), 'Redirect drives' (checkbox), 'Select redirect drives' (radio buttons for All, Only documents folder, only mobile office stick, documents and stick), 'Redirect printers' (checkbox), 'Redirect smartcards' (checkbox), 'Audio output' (checkbox), 'Multimedia Support' (checkbox), 'Redirect Clipboard' (checkbox), 'Attach to console' (checkbox), 'Use local windows client' (checkbox), 'Use alternative RDP Client (Only SBS)' (checkbox), 'Load Balancer Info' (text field), 'RDP Gateway Address' (with a dropdown), 'RDP Gateway Port' (with a dropdown), 'RDP Gateway Transport' (radio buttons for RPC, HTTP, auto), and 'Different user for RDP Gateway' (checkbox).

The host address of the terminal server, to which the remote access should be set, has to be specified in the field 'Server Address'. If the default RDP port is left unused, an alternative port can be specified in the field 'Port'.

Username and password for authentication on the terminal server can be optionally set. If the pre-allocation is correct, the login to the terminal server is performed automatically while the RDP connection is established and has not to be performed manually by the user. If only the username has been specified, it will appear in the login window and only the password has to be entered by the user.

It is also possible to set an RDP gateway via which the RDP server is reachable. For this purpose, the fields 'RDP Gateway Address', 'RDP Gateway Port' and 'RDP Gateway Transport' have to be completed in the form of the RDP configuration object. Furthermore, a separate user can be employed for authentication at the

RDP gateway. Ticking the checkbox 'Different user for RDP Gateway' opens a menu in which this user must be configured.

The form of the RDP destination object also contains the display settings. Screen resolution, color depth and window titles can be configured in these fields. Extended options can be configured in the form by ticking the corresponding checkboxes.

4.1.2 Citrix

Supported destination systems are, among others, Citrix (XenApp, XenDesktop). New Citrix destination objects can be created in the container 'Destinations'. Available options are 'Citrix Desktop' and 'Citrix Web'. The Citrix desktop object can be configured as a server, as a shared application or for the access to Storefront.

4.1.2.1 Citrix Desktop

To connect directly to a Citrix desktop, without detour via web interface login, it is required to create the object 'Destination: Citrix Desktop'.

General	Options	Proxy	Window	Application	User data	Automatic connection	Extensions	MOS Container	Admin
Name: Citrix Demo Server									
Description:									
Internal description:									
Server Address: [dropdown] Port: [dropdown]									
Use SSL: <input checked="" type="checkbox"/> Path of the Store: /Citrix/Store									
Type: <input type="radio"/> Server <input type="radio"/> Published application <input checked="" type="radio"/> StoreFront Store									
Application name:									

Select either the type 'Published application' or 'Storefront'. 'Published application' uses the 'Program Neighborhood' and only runs in XenApp up to version 7.5. 'Storefront' only runs with more recent XenApp versions.

The third type 'Server' is only used in particular cases, when the connection should not be established to a Citrix farm, but directly to a specific Citrix server. Consequently, there is no load balancing inside the farm.

In the configuration mode 'Published application', the boot stick connects to a server farm through the IP address (or group of IP addresses) specified in the field 'Server Address' to get assigned a free server. For this purpose, the application

name, respectively the desktop name of the application or the desktop to which the connection has to be established should be specified in the field 'Application Name'. The name must match the name configured in the Citrix server.

The protocol desired for the Citrix connection has to be specified in the tab 'General'. Options available are 'TCP/IP', 'TCP/IP + HTTPS' and 'SSL/TSL + HTTPS'. Here too, the port used to establish the connection can be optionally specified or the default port will be used.

Further settings can be made in the tabs 'Options', 'Proxy', 'Window', 'User Data', 'Automatic connection' and 'Extensions. These settings are only valid for the option 'Published application'.

To establish a direct connection to a desktop or an application through a Storefront store, select the type 'Storefront' in the tab 'General' of the form. It is also required to set an application name or a desktop name matching the name configured on the Citrix server. If the store is accessible through a particular path, it should be set in the field 'Path of the Store'. The connection to the store can also be established via 'HTTP' by unticking the checkbox 'Use SSL'.

If the connection is encrypted by SSL, it is additionally required to introduce the CA that signs the certificate to the boot stick in order to enable the Citrix server to check the validity of the server certificate. For this purpose, create CA objects and load the correspondent certificates. See also '4.3 | Certificates' on page 54.

Further settings can be made in the tab 'Extensions'.

4.1.2.2 Citrix Web

To establish a connection to a Citrix farm through the Citrix web interface or a NetScaler, create the object 'Destination: Citrix Webinterface'.

General			
Name			
Description			
Internal description			
Server Address		Port	
Use SSL <input checked="" type="checkbox"/>		Path of webinterface	
Citrix server			
Version for SBS		HDX Version	
Version for MOS on Windows		Version for MOS on MAC	

It is required to specify the server address of the desired web server in the tab

'General'. It is also possible to configure the port over which the connection has to be established, the path of the web interface and a potential SSL encryption.

If the connection is not established through a NetScaler, the Citrix client of the boot stick must be able to communicate directly with the server of the Citrix farm. For this purpose, specify the network within which the Citrix server is located or a list of Citrix hosts in the field 'Address of Citrixserver' so the firewall on the boot stick can be activated.

If the connection is encrypted by SSL, it is additionally required to assign the CA (signing the server certificate) to the boot stick to enable the Citrix server to check the server certificate's validity. To realize this, create the relevant CA objects and load the correspondent certificates. See also '4.3 | Certificates' on page 54.

Extended settings can be made in the tab 'Extensions'.

4.1.3 VMware

To establish a connection to VMware Horizon, create the object 'Destination: VMware View'. The IP address of the desired terminal server has to be mentioned in the field 'Server Address' and the designation of the desktop to which the connection should be established in the field 'Desktop Name'.

Various connection protocols can be selected. Options available are 'RDP', 'PCoIP' and 'BLAST'.

Username and password for authentication on the terminal server can be optionally set. If the pre-allocation is correct, the login to the terminal server is performed automatically while the connection is established and has not to be performed manually by the user. If only the username has been specified, it will appear in the login window and only the password has to be entered by the user.

4.1.4 Browser

To access a web server, create the object 'Destination: Web (Browser)'. The different browser variants can be selected in the dropdown menu of the menu item 'Layout'. In the mode 'Kiosk' the user has only access to the website defined in the field 'Start URL'. The mode 'Kiosk with URL input' allows the user to additionally access the browser's URL bar and thus also access other websites than the start URL. The 'Default' mode provides the user with an almost full browser, but without access to the file system. The mode 'Full' provides access to a fully functional browser.

The tab 'Access restrictions' allows to specifically set the websites which the user should be able to access. If the option 'Allow all http and https access' is enabled, the user is entitled to call up any website. This can be restricted with the list 'Access limitations'. The list allows to interdict access to particular IP addresses and domains. Conversely, it is also possible to use the list to allow access to certain IP addresses, although a general access has been prohibited by disabling the option 'Allow all http and https access'.

Furthermore, the tab 'Access restrictions' allows to authorize or ban plugins such as RDP or Java. If the Java plugin has been enabled, it is required to additionally specify the websites allowed to perform Java applications in the submenu 'URLs enabled for Java'.

The tab 'Modify browser' allows further settings, such as the import of Firefox settings in the field 'Preferences'.

4.1.5 Hotspot

To allow internet access via hotspot, it is required to configure a web browser in 'Kiosk' mode as destination and to assign a start URL (e.g. the company website). After starting the boot stick, a connection to WLAN is established through the network settings. It is then possible to start the browser and log into the hotspot. The hotspot login has been successful if the website specified for start URL is opened.

4.2 Users

Users are located below the container object 'User'. Users are employed to control access at different points. On the one hand, the access to the administration interface can be authorized in whole or in part, on the other hand, the user object defines the destinations (terminal server etc.) that may be accessed from the boot stick.

In the delivery state, the user "admin" is predefined and endowed with administrator privileges. Administrators have an unrestricted access to all configuration objects und features.

A new user can be created by right-clicking on the container 'User' and then selecting the configuration object 'User' in the menu item 'New'.

Use the tab 'General' to assign a name to the user. By ticking the checkbox 'Admin access' or 'Access to admin interface', the user can be endowed with administrator privileges.

The screenshot shows the 'General' configuration tab for a user. The tab is highlighted in yellow. Below the tab are several sub-tabs: Spam filter, Mail filter, Mobile Office, Virtual Web, Authentication, and Certificates. The main form area contains the following fields and options:

- Name:** A text input field.
- Login:** A text input field.
- Description:** A text input field.
- Surname:** A text input field.
- Department:** A text input field.
- Password:** A text input field.
- Password re-enter:** A text input field.
- Admin access:** A checkbox with an information icon.
- Do not hash password:** A checkbox.
- Access to admin interface:** A checkbox with an information icon.
- Role:** A dropdown menu with a downward arrow.

For a more detailed description on how to assign privileges: See also '6.7.2 | How to assign roles to users' on page 98.

It is also required to set a password so the user will later be able to authenticate at the administration interface.

4.3 Certificates

The administration interface allows to issue CA certificates and X-509 server certificates. These are stored in the folder 'Certificates'.

4.3.1 CA certificates

The Certificate Authority (CA) allows to create and sign certificates. The use of public keys offers the possibility to check whether a certificate has truly been issued by a specific CA.

A CA certificate, like all other configuration objects, can be created in different ways, for example by right-clicking on the folder 'Certificates' in the tree and selecting 'New' > 'CA Certificate'.

Once a new CA has been set, the CA certificate can be created by selecting 'Certificate creation' and then the menu item 'Create automatically'. Further parameters, such as validity, subject and key size, can be selected. Alternatively, the certificate will be created with default settings, for example with a key size of 2048 bits.

General		Alternate names	Usage	History	Certificate	Admin
Name <input type="text"/>						
Description <input type="text"/>						
Certificate creation		---		Status		certificate revoked
Sign certificate with		<input type="radio"/> self-signed <input checked="" type="radio"/> CA		CA		ca test
Validity		365 days				
Subject <input type="text"/>						
Issuer <input type="text"/>						
Keysize		2048 Bits		Encrypt private key		encrypted and unencrypted
Signature hash algorithm		sha256				
Fingerprint <input type="text"/>						
Valid from				Valid to		
Certificate		Upload		Certificate as PKCS #7		
Private key		Upload		Certificate as PKCS #12		
Certificate request		Upload		Certificate as PEM		
Assign smartcard		<input type="text"/>				
Smart card certificate		<input checked="" type="radio"/> none <input type="radio"/> Smart card <input type="radio"/> System				
Smart card enrollment		Start		Smart card certificate select		Select
Smartcard certificate info		<input type="text"/>		IE Smart card enrollment		Start
Windows CSP Name <input type="text"/>						

4.3.1.1 Parent CA

This option allows to select a superordinate CA which, in turn, can be used to sign the CA certificate to be created. The parent CA must have been created and generated (or uploaded) beforehand.

4.3.1.2 Validity

Indicates the validity of the certificate in days.

4.3.1.3 CRL distribution point URL

Specifies an HTTP or LDAP URL via which the CRL (certificate revocation list, a list of certificates that have been revoked) can be loaded. This URL will be added to any certificate signed by the CA. While checking a certificate, the CRL can be requested to control whether the certificate has been withdrawn by the CA.

4.3.1.4 Subject

Allows to specify the subject of the CA certificate. If nothing is mentioned, the subject will be automatically generated from its position in the tree.

Clicking on 'Apply' prompts a popup in which a password for the private key can be specified.

Instead of creating a CA certificate through the administration interface, certificates can also be uploaded from an external certification authority.

A certificate previously generated can be withdrawn in the pull-down menu under 'Certificate creation'. The field 'Status' shows the current status of the CA certificate, for example 'Certificate generated' or 'Certificate revoked'.

The menu item 'Request CA password' allows to define for what kind of actions the password will be required. Options available are: 'Always', 'When created', 'Never' and 'Not for CRL'.

When the option 'When created' is enabled, the password is only required when new certificates are generated. When 'Not for CRL' is enabled, no password will be required when generating the CRL.

The subsequent modification of this setting requires the password.

4.3.1.5 History

The tab 'History' allows to retrace when the certificate has been created and, if applicable, revoke it.

4.3.2 X-509 server certificate

X-509 server certificates are created in the same way than CA certificates.

After the creation of the certificate object, a server certificate can be created through the pull-down menu 'Certificate creation' > 'Create automatically'.

The field 'Sign certificate with' allows to specify whether the certificate should be self-signed or signed by a CA. The field 'CA' offers a range of certificate authorities that can be used to sign the certificate.

Further parameters like validity, subject and key size can be selected. It is also possible to define whether the private key should be 'encrypted and unencrypted', 'only encrypted' or 'only unencrypted'.

Clicking on 'Apply' opens a popup in which the password for the private key can be specified.

After setting the password for the private key, it is required to set the password for CA certificate, provided that the option 'CA' has been enabled under 'Sign certificate with' and that the respective CA has been set to require a password when a certificate is generated.

4.3.2.1 Alternate names

The tab 'Alternate names' allows to assign e-mail addresses, DNS names and/or URLs to a certificate.

The screenshot shows the 'Alternate names' tab selected in a configuration interface. The interface has a yellow header bar with tabs: General, **Alternate names**, Usage, History, Certificate, and Admin. Below the tabs, there are four input fields, each with a label on the left and a text area on the right:

- E-Mail(s)**: A text input field.
- DNS name(s) / IP address(es)**: A text input field.
- URI(s)**: A text input field.
- OtherName**: A text input field.

4.3.2.2 Usage

The tab 'Usage' allows to define the purpose of the certificate more precisely.

The screenshot shows the 'Usage' tab selected in the configuration interface. The interface has a yellow header bar with tabs: General, Alternate names, **Usage**, History, Certificate, and Admin. Below the tabs, there is a 'Usage' dropdown menu with a downward arrow. At the bottom of the tab, there are two buttons: 'Apply' and 'Actions' with a right-pointing arrow.

4.3.2.3 History

The tab 'History' allows to retrace when the certificate has been created and, if applicable, revoke it.

5 Boot stick configuration and enrolment

5.1 Local configuration vs. central management

The configuration of the ECOS SECURE BOOT STICK can be performed either locally on the boot stick itself or through the central management. The advantage of a central management is that changes of configuration don't have to be made on every single boot stick. They are made only once in the central management and then automatically transferred to all boot sticks. Besides, for a simplified management of a large number of boot sticks, it is also possible to create central boot stick templates that will hand down their configuration to the different boot sticks. Furthermore, the automatic creation of boot stick configurations from other directory services via directory synchronization is possible too.

The central management is highly recommended for the usage of the ECOS SECURE BOOT STICK.

5.2 ECOS SECURE BOOT STICK configuration

In its delivery state, ECOS SECURE BOOT STICK is not configured and has to be configured or personalized for its intended usage. For this purpose, create a configuration for the boot stick in the central management and transfer it to the boot sticks via Easy Enrollment.

5.2.1 Services required by the ECOS SYSTEM MANAGEMENT APPLIANCE (SMA)

ECOS SYSTEM MANAGEMENT APPLIANCE requires the following services for the management of ECOS SECURE BOOT STICK (SBS):

- The Radius service is necessary to verify the activations codes. The software update server is required for Easy Enrollment and provides the boot sticks with software updates. See also '6.2 | Updates' on page 80. These services can be created easily in the ECOS SYSTEM MANAGEMENT APPLIANCE by just ticking the checkbox 'Start'.
- Also required is the ECOS System Connector which constitutes the fundamental link between appliance and boot sticks for both the rollout procedure and later configuration changes. Not only do the boot sticks connect to it, it also forwards requests from the sticks to the appliance.

5.2.2 ECOS System Connector for SBS

The ECOS System Connector is created on the ECOS appliance in the container 'VPN'. The connector is enabled by ticking the checkbox 'Start'.

The screenshot shows the configuration page for the 'ECOS System Connector'. The 'General' tab is selected. The 'Name' field is 'ECOS System Connector'. The 'Start' checkbox is checked. The 'Local address for external access' and 'Local address for access from the LAN' are both set to 'LAN@bbtest7g2 (Dev: 10.161.200.18)'. The 'Port' and 'Listen address' are both set to '80'. The 'Use SSL for proxy' checkbox is unchecked. The 'Certificate' field is empty. The 'Name of stick for activation' is empty. The 'Logging' dropdown is set to 'Info'. The 'Use DNS name instead of IP address' checkbox is unchecked. The 'Servertimeout' field is empty. The 'Version of MOS' dropdown is set to 'V4'. The 'URL for update from V4 to V5' field is empty. The 'Authenticated user CAs' field is empty. The 'SBS EasyEnrollment Configuration' field is empty. The 'Certificate Subjects allowed for EasyEnrollment' field is empty. The 'VPN for EasyEnrollment' dropdown is set to 'VPN'. The 'Servertimeout' field is empty. There is a 'Download' link next to the 'SBS EasyEnrollment Configuration' field.

The ECOS System Connector requires a network address accessible by LAN/WAN and which should be specified in the field 'Local address for external access'. The connected boot sticks will use this address to direct their requests to the appliance. Also, this address is required to generate and verify the activation codes of the boot sticks.

In addition to the 'Local address for external access', it is also possible to specify a 'Local address for access from the LAN'. Once both addresses are set, the boot stick will send them a request on connection establishment and connect to the one answering first.

The field 'Port' allows to configure the port through which the boot sticks should address the ECOS System Connector. If not port is set, the default port will be 909.

An activation code containing the encoded address of the ECOS System Connector will be later required to personalize the boot stick during Easy Enrollment. It's the address specified in the field 'Local address for external access' of the ECOS System Connector. The boot stick uses this address to connect to the ECOS System Connector during Easy Enrollment. If the field 'Local address for external access' of the ECOS System Connector is left empty, the address specified in the field 'Local address for access from the LAN' will be used to generate the activation code.

For a successful Easy Enrollment, the address encoded in the activation code must be accessible by the boot stick. If the ECOS SYSTEM MANAGEMENT APPLIANCE is, for example, protected by a firewall making Network Address Translation (NAT) a management appliance, it is also necessary to specify the external firewall address.

When changing the address in the ECOS System Connector, it may be necessary to regenerate the existing Easy Enrollment codes.

5.2.3 How to configure ECOS System Connector for SBS with smart card

For the usage of SMA with SBS and smart card, further configuration settings will be required in addition to those explained by '5.2.2 | ECOS System Connector for SBS' on page 60.

5.2.3.1 How to configure CA certificates for usage with smart card

If the smart card is managed by the ECOS appliance, the creation of a new CA certificate is required. See also '4.3.1 | CA certificates' on page 55.

For an already existing smart card, it is necessary to configure on the SMA the CA certificates of the certificates used on the smart card to allow an authentication on the ECOS system via smart card certificate.

For this purpose, create a new container with a random name by selecting 'Certificates' and then 'New' to configure all CA certificates required for usage.

The easiest way to configure the different certificates is to create a new certificate object with a random name and a numeral suffix in 'Certificates' > 'New' > 'Certificates & smart cards' > 'CA certificate' (for example 'CA-Cert 1'). This CA

certificate object can then be pasted anywhere with the menu item 'Duplicate' and will automatically get a progressive numbering.

After creating the CA certificate object, it is necessary to upload the respective certificate into the tab 'General' > 'Certificate' > 'Upload' of the certificate object.

5.2.3.2 Specific configurations of the ECOS System Connector for smart card usage

The created CA certificates must be configured in the field 'Root certificate user authentication' by selecting the name of the created CA certificate or container (group) from the list.

Also, the certificates admitted for authentication must explicitly be configured by setting the subject DN. Thus, it is possible to restrict the users admitted for login in a more fine-grained way. For this purpose, configure a filter expression in the field 'Certificate subjects admitted to Easy Enrollment'. For a better understanding of the syntax of the filter expression, a few examples in the following:

Syntax	Example
C=DE,O=Company xyz,OU=Sales,CN=*	all employees of the company xyz belonging to the organization unit 'Sales'
C=DE,O=Company xyz,OU=*,CN=*	all employees of the company xyz and from Germany
C=DE,O=Company xyz,OU=Sales,CN=* C=DE,O=Company xyz,OU=Production,CN=*	all employees of the company xyz, from Germany, belonging to the organization units 'Sales' or 'Production'

Table 5.1 Configuration example of a filter

All DN components are required and can be selected by wildcard (*). There is no general wildcard for the whole DN. A logic or (|) allows to combine several terms.

5.3 SBS Personalization

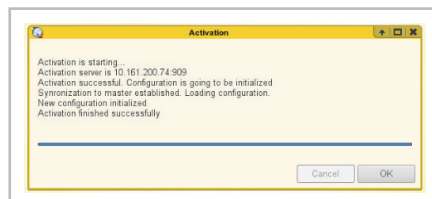
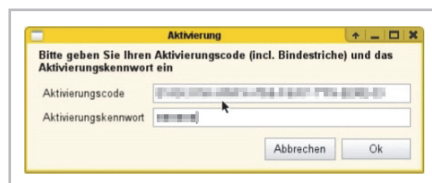
ECOS SECURE BOOT STICK is activated and personalized by assigning the

configuration of the boot stick object to the physical USB drive either via Easy Enrollment or by exporting the configuration from ECOS SYSTEM MANAGEMENT APPLIANCE to the boot stick.

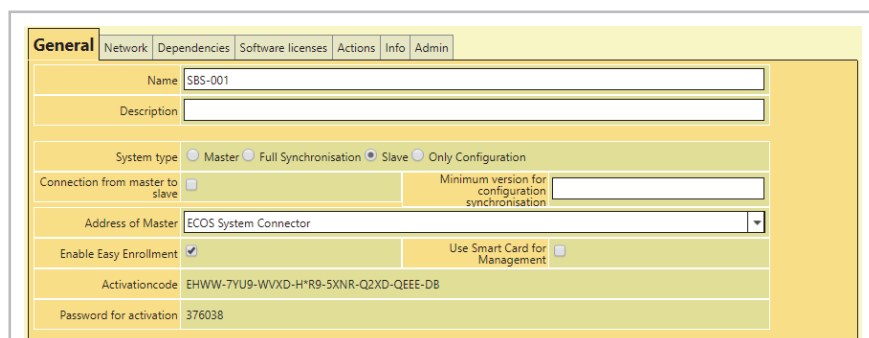
5.3.1 Easy Enrollment

For Easy Enrollment, it is necessary to connect the boot stick to a computer and start it. In the delivery state, this prompts an input mask requesting the activation code and the activation password.

To generate the activation code, it is necessary to tick the checkbox for Easy Enrollment in the boot stick object on the appliance.



The activation code will only be generated once the checkbox for Easy Enrollment has been ticked and the setting applied.



After entering the activation code on the boot stick, the stick will contact the management and download automatically all required configuration settings from the correspondent master server. For this purpose, the IP address of the

management is encoded in the activation code of the Easy Enrollment. It comprises the address specified in the field 'Local address for external access' of the ECOS System Connector. For further information about the configuration of the ECOS System Connector: See also '5.2.2 | ECOS System Connector for SBS' on page 60.

For the success of Easy Enrollment, the boot stick must be able to establish a connection to the ECOS MANAGEMENT APPLIANCE.

If the option 'Protect Bootstick with Password' has been enabled in the boot stick configuration, the user must set a boot password during Easy Enrollment. This password will be requested every time the boot stick is started. The user can change the boot password in the boot stick menu later.
For more information cf. ECOS SECURE BOOT STICK User Guide.

In case the boot password should need to be reset, for example because the user can't remember it, Easy Enrollment can be performed again. To do so, press the key combination F12+Enter in the dialogue into which you normally type the boot password. The boot stick will then start without configuration. Easy Enrollment can now be performed again. It can also be started by clicking on the ECOS icon on the bottom left of the taskbar and select 'System'> 'Activation'.

The activation code for Easy Enrollment is only valid once. If it should become necessary to perform a new Easy Enrollment on an already activated boot stick, a new activation code must be generated through the management appliance first.

5.3.2 Easy Enrollment with smart card - SBS [SE] and SBS [SX] only

The authentication of the management connection by smart card requires to enable the option 'Smartcard usage for management' under 'Bootstick'. This is a non-adjustable pre-configuration in the BSI-approved SBS version.

In case of usage with already existing smart cards, the SBS must be pre-configured in order to recognize the address of the SMA. This can be done directly on delivery by ECOS or later manually. A suitable pre-configuration can be downloaded from the system connector and then directly uploaded into the boot stick through the boot stick configuration object. The end user can then start Easy Enrolment by simply plugging in the smart card after booting the SBS.

If the smart card is made available by the ECOS management, the relevant certificates for the boot stick must be created first to finally roll them out onto the smart card.

For this purpose, new certificates must be created under 'Bootsticks' > 'Certificates'. One certificate respectively is required by the management connection, for the VPN connection and for the encryption of the SBS. See also '4.3.2 | X-509 server certificate' on page 57.

Following settings are required in the certificate objects: The field 'Certificate creation' must be set to automatic and the option 'Smart card certificate' enabled. These settings allow to later roll out the certificates onto a smart card.

Additionally, the option 'SBS authentication' must be enabled under 'Usage' > 'Certificate usage' for the authentication of the management connection. This way, the SBS configuration for Enrolment will be embedded in a certificate extension.

Clicking on 'Smartcard Enrollment' in the SBS object will start the certificate enrolment tool responsible for the rollout of the certificates onto the smart card. For this purpose, the smart card must be connected to the Windows computer on which the browser containing the administration interface has been called up.

If the smart card hasn't been initialized yet, this will be performed automatically by requesting a PIN and a PUC for the smart card. It is also possible to reinitialize the smart card during the enrolment by selecting under 'Smartcard Init' the option 'Format'.

5.3.3 Export

Instead of Easy Enrollment, an ECOS SECURE BOOT STICK can also be activated and personalized by exporting the configuration manually from the management appliance.

If a smart card is used for authentication of the management connection, the activation by export is impossible and can only be realized through Easy Enrollment.

In this case, it is first necessary to delete the firewall on the boot stick. To do so, call the start menu through the ECOS icon at the bottom left of the taskbar. Open 'System' > 'Console', login with the username 'setup' and the password set for maintenance. If no password has been set, the default password is 'bb5000'. This will prompt a splash screen. Press any key to access the pulldown menu. Pressing the key 'F' will delete all firewall rules.

Select the action 'Configuration export' from the tab 'Action' in the boot stick object of the management appliance. This opens a submenu in which to insert the address of the destination system, the port of the administration interface and the admin user with the password. The configuration export will be started by clicking on the button 'Start'.

The configuration export is only possible if the management appliance is able to access the boot stick by HTTPS connection **and** if, conversely, the boot stick is able to contact the management appliance through the port specified in the ECOS System Connector.

5.4 SBS VPN

To access destinations in an insecure network, for example the internet, a VPN connection is usually necessary. For this purpose, ECOS SECURE BOOT STICK (SBS) contains integrated IPsec and SSL VPN clients. Furthermore, the boot stick supports Java for a clientless VPN connection by browser.

It is thus possible to establish a connection to the VPN gateways of all leading manufacturers. ECOS SYSTEM MANAGEMENT APPLIANCE and ECOS SECURE GATWAY APPLIANCE, too, can be used as VPN gateways and authentication servers for ECOS SBS.

The desired VPN client can be selected and created in the container 'VPN' under the boot stick object by right-clicking on 'New'. Different settings are required in the VPN client object depending on the VPN type.

General		Advanced	Encryption / compression	Proxy	Shared Secret	Admin
Name	<input type="text"/>	Start	Off			
Description	<input type="text"/>		On Demand			
Start connection by profile	<input type="text"/>		Only Remote			
			Start			
Local address	<input type="text"/>	Bind to local address	<input type="checkbox"/>			
Remote address	<input type="text"/>	Select random remote host	<input checked="" type="checkbox"/>			
Local subnet	<input type="text"/>					
Local certificate	<input type="text"/>	CA certificate	<input type="text"/>			
Special options						
Don't bind tunnel to local port	<input type="checkbox"/>	Enable Ping timeout only when remote address available	<input type="checkbox"/>			
Time between tcp reconnects	<input type="text"/> Sec	Max. time for resolving dns	<input type="text"/> Sec			
Remote name	<input type="text"/>	Log Level	3			
Redirect Default Route	<input type="checkbox"/>					
Local redirect	<input type="checkbox"/>	Alternative route	<input type="checkbox"/>			

5.4.1 Starting the VPN connection

Through the VPN client object can be configured when the VPN connection should be established. The VPN tunnel can be build up automatically when starting the boot stick or 'On Demand'. In this case, the VPN tunnel will only be established when an application (destination) is started that needs VPN. The destination or a group of destinations can be specified in the field 'Start connection by profile'. If the field is left empty, all destinations will start the VPN connection. If something has been selected, the VPN connection will only be built up when the selected destinations are started.

5.4.2 IPsec

Internet Protocol Security (IPsec) is a protocol suite allowing a secured communication via Internet. To secure the boot stick's VPN connection to the VPN gateway with IPsec, the boot stick must contain a configured IPsec client. This client must be created in the container 'VPN' below the boot stick object. Option available are 'IPsec aggressive mode connection', 'IPsec NCP client', 'IPsec Shrewsoft client' and 'IPsec client version'.

5.5 SBS optional features

5.5.1 Boot loader

The service 'Boot loader' allows to control the start behavior of ECOS SECURE BOOT STICK and to restrict the user access to the boot menu.

General		Admin
Name	<input type="text"/>	Start <input type="checkbox"/>
Description	<input type="text"/>	
Enable password protection	<input type="checkbox"/>	Hide bootmenu <input type="checkbox"/>
Password protection	<input type="text"/>	
Disable splash screen	<input type="checkbox"/>	Disable alternative splash screen <input type="checkbox"/>
ACPI Settings	On <input type="button" value="v"/>	
Activate PC Express Hotplug	<input type="checkbox"/>	Activate PCI Express hotplug fallback <input type="checkbox"/>
Disable local display	<input type="checkbox"/>	Enable Num-Lock <input type="checkbox"/>

5.5.2 Mass storage

If mass storage devices, such as USB flash drives or CD-ROM, have to be integrated into a remote session, they must be activated separately. By default, the user has no access from the terminal server to the mass storage device. If such an access is desired, it is necessary to create the correspondent storage object in the administration interface below the boot stick. To do so, right-click on the boot stick object or the container 'Mass storage' below it to open the tree menu and select the desired type of mass storage under 'New' > 'Periphery'. Options available are CD-ROM and USB flash drives.

To allow access to a storage device, it is necessary to tick the checkbox "Start" in the object's form.

In the case of a USB stick, it is possible to specify in the USB object if access should be allowed to all USB flash drives. Alternatively, it is possible to allow or ban access of single sticks according to manufacturer, product series or serial numbers. It is also possible to distinguish between read and write access.

General		Admin
Name	<input type="text"/>	Start <input type="checkbox"/>
Description	<input type="text"/>	
Search for USB storage	Select	
Device Information		
Manufacturer	<input type="text"/>	Product <input type="text"/>
Device discovery		
Manufacturer ID	<input type="text"/>	Manufacturer required <input type="checkbox"/>
Product ID	<input type="text"/>	Product required <input type="checkbox"/>
Serial number	<input type="text"/>	Serial number required <input type="checkbox"/>
Write access	<input type="checkbox"/>	Deny access <input type="checkbox"/>

5.5.3 Printer

Similarly to mass storage devices, the usage of printers in the remote session must be activated. For this purpose, a printer object must be created below the boot stick object. To do so, use the menu that appears when right-clicking on the boot stick object or on the container below named 'Printer'. The printer object can be found under 'New' > 'Periphery'.

ECOS SECURE BOOT STICK itself contains no driver for printers. It is therefore necessary to install the suitable printer driver on the terminal server. The boot stick tells the terminal server which printer is connected in order to allow the selection of the correct driver once the connection to the terminal server is being established. In general, it is sufficient to install a couple of universal drivers from the corresponding printer manufacturer to be able to operate most of the printer models.

Printers can be configured automatically or manually.

The printer name in the terminal server session is the name specified in the printer object.

The port of the desired printer must be stated in the printer object. If the printer is connected locally, options available are 'Parallel port' and 'USB'. If you wish to use a network printer, select 'URI' and then specify the printer's URI.

If the printer is configured manually, it is necessary to specify the driver name in the field 'Driver name'. The name must be identical to the name of the printer driver on the terminal server (blank spaces included). This name can be found in Windows printer settings. If the configuration is performed automatically, the field should be left empty.

By ticking the checkbox 'Manage printers automatically', the field 'Driver name' will be filled automatically according to the connected printer and the printer object will be activated (respectively deactivated when removing the printer). The printer must be connected by USB.

General		Admin
Name	<input type="text"/>	Start <input checked="" type="checkbox"/>
Description	<input type="text"/>	
Driver name	<input type="text"/>	Printer map <input type="text" value="USB Printer"/>
Default printer	<input type="checkbox"/>	Manage printer automatically <input checked="" type="checkbox"/>
Port	<input type="text" value="USB Printer"/>	USB Printer
USB Path	<input type="text"/>	Reset <input type="checkbox"/>

To make the printer available from the terminal server, it is also necessary to tick the checkbox 'Start' in the object's form.

General		Admin
Name	<input type="text"/>	
Description	<input type="text"/>	
Internal description	<input type="text"/>	
Server Address	<input type="text"/>	Port <input type="text"/>
User name	<input type="text"/>	Password <input type="text"/>
Domain	<input type="text"/>	
Screen resolution	<input type="text"/>	Color depth <input type="text" value="24 Bit"/>
Keyboard layout	<input type="text" value="English (USA)"/>	Window title <input type="text"/>
Hide window decoration	<input type="checkbox"/>	Compression <input checked="" type="checkbox"/>
Network level authentication	<input type="checkbox"/>	Activate cache <input checked="" type="checkbox"/>
Multimonitor support	<input type="checkbox"/>	Disable encryption <input type="checkbox"/>
Select redirect drives	<input checked="" type="radio"/> All <input type="radio"/> Only documents folder <input type="radio"/> only mobile office stick <input type="radio"/> documents and stick	
Redirect printers	<input checked="" type="checkbox"/>	Redirect smartcards <input type="checkbox"/>
Redirect Clipboard	<input type="checkbox"/>	Attach to console <input type="checkbox"/>
Load Balancer Info	<input type="text"/>	
RDP Gateway Address	<input type="text"/>	RDP Gateway Port <input type="text"/>
RDP Gateway Transport	<input checked="" type="radio"/> RPC <input type="radio"/> HTTP <input type="radio"/> auto	
	Different user for RDP Gateway <input type="checkbox"/>	

Since the name of the printer transmitted by USB doesn't automatically correspond to the driver name, the relevant driver name can be generated from the printer name through the driver allocation table. For this purpose, the field 'Driver allocation table' must refer to an allocation table. In this case, instead of using the driver name stated in the field 'Driver name', the driver name assigned by the allocation table will be sent to the terminal server.

5.6 Inheritance

When several boot sticks with the same configuration are needed, it is recommendable to set up a basic configuration from which the boot stick objects will inherit their configuration. Thus, settings must be done only once and even later modifications are only required once and centrally.

In the first step, the basic configuration of a series of boot sticks is the same than the configuration procedure of a single stick. Right-clicking on the container 'Boot sticks' opens a menu in which to select 'New' and then an ECOS system object. In the tab 'General' select the type 'Only Configuration' instead of the system type 'Slave'. It is now possible to create configuration objects that are identical to all/ many boot sticks below the basic configuration object, for example the software update service or VPN clients as far as they have identical settings for all boot sticks.

The screenshot shows the 'General' tab of a configuration window. The 'System type' dropdown menu is open, and 'Only Configuration' is selected and highlighted with a red rectangle. Other visible fields include 'Name' (Testbootstick), 'Description', 'Local user' (demo-user), and 'Type of database' (CDB). There are 'Apply' and 'Actions' buttons at the bottom right.

When creating a new boot stick it is now only necessary to specify the desired basic configuration in the tab 'Dependencies' and the field 'Based on'. Thus, the boot stick automatically acquires the configuration of all services and objects located below the basic configuration.

The screenshot shows the 'Dependencies' tab of the same configuration window. The 'Based on' dropdown menu is set to 'Testbootstick'. There are also 'Add to' and 'Add only to the first available host' options. The 'Add only to the first available host' checkbox is unchecked.

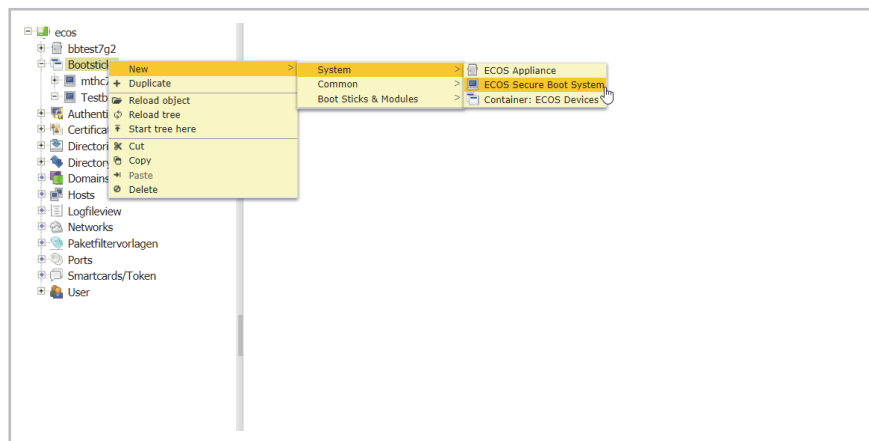
If the configuration of a boot stick should differ in some points from the basic configuration, it is necessary to create corresponding configuration objects below the actual boot stick object. Thus, the relevant settings in the basic configuration will be overridden.

It is possible to create several objects of the same type from some object types, for example network interfaces. If such an object has been defined in the basic class and below the boot stick object, the object in the basic class will not be overridden and both objects will exist next to each other.

It is possible to inherit the settings from several basic configurations at the same time. If different parameters have been set in the basic configuration, the boot stick will acquire the settings of the basic configuration located on top in the tab 'Dependencies' of the boot stick object.

5.6.1 Create/configure SBS objects

To create a new ECOS BOOT STICK, select a configuration object type 'System' by right-clicking on the container 'Boot sticks' in the left navigation bar under 'New'.



The name of the new boot stick must be specified in the tab 'General'. It is now necessary to select the option 'Slave' in the field 'System type'. A submenu appears. The connection to the ECOS SYSTEM MANAGEMENT APPLIANCE can be configured in the field 'Address of Master'. State here the previously configured ECOS System Connector. All parameters required for a connection to the appliance, such as IP address and port, will then be acquired from the ECOS System Connector. Alternatively, it is also possible to state directly the IP address of the master. In this case, the port is fixed to 909.

The screenshot shows the 'General' tab of the configuration interface. The 'Name' field is set to 'Testbootstick'. The 'System type' is set to 'Slave'. The 'Address of Master' is set to 'ECOS System Connector'. The 'Enable Easy Enrollment' checkbox is checked. The 'Local user' is set to 'demo-user'. The 'Protect Bootstick with Password' is set to 'No password'. The 'Type of database' is set to 'CDB'. The 'Smart Card Init' is set to 'No'. The 'Smart card enrollment' button is labeled 'Start'. The 'Apply' button is highlighted with a red box.

Tick the checkbox 'Enable Easy Enrollment' to activate it. After clicking on 'Apply', activation code and password will be generated automatically. For more information on Easy Enrollment: See also '5.3.1 | Easy Enrollment' on page 63.

It is also necessary to complete the fields 'Local Admin User' and 'Local user' that will be described in the following.

General	Network	Dependencies	Software licenses	Actions	Info	Admin
Name: Testbootstick						
Description:						
System type: <input type="radio"/> Master <input type="radio"/> Full Synchronisation <input checked="" type="radio"/> Slave <input type="radio"/> Only Configuration						
Connection from master to slave: <input type="checkbox"/> Minimum version for configuration synchronisation:						
Address of Master: ECOS System Connector						
Enable Easy Enrollment: <input checked="" type="checkbox"/> Use Smart Card for Management: <input type="checkbox"/>						
Activationcode: EHWW-7YU&-WVXD-H*8B-3T4D-NXCR-QR4A-F5						
Password for activation: 973131						
Local Admin User: admin Local user: demo-user						
Protect Bootstick with Password: <input checked="" type="radio"/> No password <input type="radio"/> Set by user during EasyEnrollment						
Type of database: CDB Start VPN for Management Connection: <input type="checkbox"/>						
Smart Card Init: <input checked="" type="radio"/> No <input type="radio"/> Format <input type="radio"/> New Pin Smart card enrollment: Start						
<input type="button" value="Apply"/> <input type="button" value="Actions"/>						

Enable Easy Enrollment	<input checked="" type="checkbox"/>
Activationcode	E*****5
Password for activation	973131

The option 'Protect Bootstick with Password' specifies whether a password authentication will be required upon every start of the boot stick. When the option 'Set by user during Easy Enrollment' is set, the user will be required to state a password during the activation procedure of the boot stick.

The configuration of boot stick objects can be set inheritable in the tab 'Dependencies'. This means that all settings of a basic configuration will automatically apply to the boot stick object. For more information about 'Inheritance of boot stick configurations': See also '5.6 | Inheritance' on page 72.

General	Network	Dependencies	Software licenses	Actions	Info	Admin
Based on: <input checked="" type="radio"/> mthc7g						
Add to: <input checked="" type="radio"/>						
Add only to the first available host: <input type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Actions"/>						

5.7 Information about the management connection

When an ECOS SECURE BOOT STICK is started on a computer connected to the network, the boot stick will automatically connect to the management. The connection can be established through a random TCP port specified in the configuration form of the ECOS System Connector. See also '5.2.2 | ECOS System Connector for SBS' on page 60..

The connection to the management is encrypted, based on the SSH protocol. It is not possible to establish a connection between management and boot stick via proxy as the ECOS SYSTEM MANAGEMENT APPLIANCE and the ECOS BOOT STICK authenticate each other to warrant a secure connection and exclude any manipulation.

A master-slave relation exists between the ECOS SYSTEM MANAGEMENT APPLIANCE and ECOS SECURE BOOT STICK. As soon as they are connected to each other, the configuration of the slave will be handed automatically from master to slave. Only configuration objects necessary for the slave will be handed down. Modifications become immediately effective on transmission.

It is possible to modify the configuration locally on the boot stick through a local admin user. This option is not intended for actual configuration purposes on the boot stick and should only be used when modifications have to be made while there is no connection to the management appliance. Modifications performed on the slave will not be transmitted to the master and overridden by the settings stored on the master during the next master-slave contact.

5.8 Destinations

To allow a remote access from a boot stick to a terminal server or another destination system, it is necessary to create destinations. Destinations are those systems to which the user actually gets access. The data required for the connection establishment are to be specified in the corresponding configuration objects. For more information about the different destination systems and their configuration: See also '4.1 | Destinations (connection profiles)' on page 48.

The locally defined user of the boot stick determines what kind of destinations can be accessed with this boot stick. For more information about local users: See also '5.9 | Local admin and local user' on page 77.

5.9 Local admin and local user

The boot stick must be assigned a local admin user and a local user in the boot stick object under the tab 'General'. These have different roles. The local admin user can modify configuration settings locally through the web interface of the boot stick, independently from ECOS SYSTEM MANAGEMENT APPLIANCE. This is necessary for maintenance purposes when there is no access to the appliance. For a more detailed description of the master-slave relation: See also '5.7 | Information about the management connection' on page 76..

Local admin users can only be those users who have either a permission for 'Admin access' or 'Access to admin interface'. These permissions can be given by ticking the respective checkboxes in the tab 'General' of the user object. Also, it is necessary to specify a password for authentication in the administration interface.

General		Spam filter	Mail filter	Mobile Office	Virtual Web	Authentication	Certificates
Login	Destinations	Personal data	Certificate	Admin			
Name	admin			Login	admin		
Description							
Surname	ECOS System Standard Benutzer			Department			
Password	*****			Password re-enter	*****		
Admin access	<input checked="" type="checkbox"/>			Do not hash password	<input type="checkbox"/>		
Access to admin interface	<input type="checkbox"/>			Role	---		
<div>Apply</div> <div>Actions</div>							

Unlike the local admin user, the local user needs no admin rights and no password for authentication in the administration interface. The local user determines which destinations should be accessible for ECOS SECURE BOOT STICK. Destinations are those systems to which the user actually needs access, for example Microsoft Terminal Server or a Citrix farm. For a more detailed description of available destinations and their configuration: See also '4.1 | Destinations (connection profiles)' on page 48.

The destination to which the user and his boot stick have access are defined in the tab 'Destinations' of the user object. Existing destination objects can be selected in the table 'Destinations' and activated for the different products by ticking the checkboxes for 'Secure Boot', 'Mobile Office' and 'Virtual Web', respectively. It is also necessary to tick the checkboxes 'Active' and 'Secure Boot' in the destination table of the user object to give the user access to a destination of ECOS SECURE BOOT STICK.

The destinations that have been activated for the respective user will be displayed in the pull-down menu when the boot stick is started. The destinations available can be modified by activating or deactivating, respectively adding or deleting destinations in the table of the user form.

If various boot sticks should receive the same selection of destinations, it is possible to assign them the same local user. In this case, the local user corresponds to a user group with the same properties.

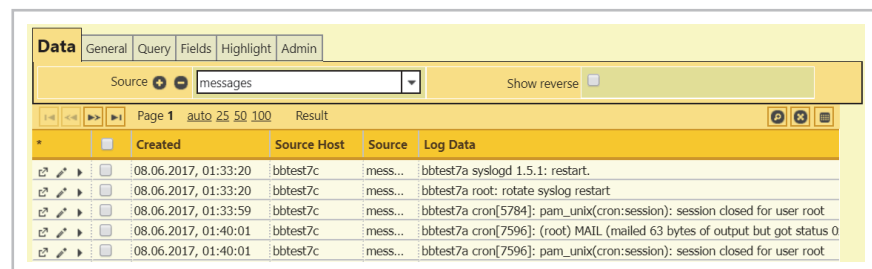
Vice versa, it is not possible to assign one boot stick to more than one user. This means that a particular boot stick only provides access to those destination systems that have been activated for the local user. To customize the range of destination systems to which the boot stick will be able to connect, it is necessary to either modify the approved destination systems in the user form in the tab 'Destinations' or assign the boot stick another user in the tab 'General'

6 Further topics

6.1 Log files

6.1.1 View/evaluate

For a neat view of the log files, use the log file display object. It can be created by right-clicking on a random container under 'New' > 'Data'. The process, of which the desired log file entries shall be displayed, should be specified in the field 'Source' of the tab 'General' in the log file display object. It is also necessary to assign a name to the log file display object in the tab 'General'. Clicking on 'Search' or 'Apply' will display the respective log file entries in tabular form.



The screenshot shows a web interface for displaying log files. At the top, there are tabs: 'Data', 'General', 'Query', 'Fields', 'Highlight', and 'Admin'. The 'Data' tab is active. Below the tabs, there is a 'Source' dropdown menu set to 'messages' and a 'Show reverse' checkbox. Below this, there is a table with the following columns: 'Created', 'Source Host', 'Source', and 'Log Data'. The table contains five rows of log entries.

	Created	Source Host	Source	Log Data
	08.06.2017, 01:33:20	bbtest7c	mess...	bbtest7a syslogd 1.5.1: restart.
	08.06.2017, 01:33:20	bbtest7c	mess...	bbtest7a root: rotate syslog restart
	08.06.2017, 01:33:59	bbtest7c	mess...	bbtest7a cron[5784]: pam_unix(cron:session): session closed for user root
	08.06.2017, 01:40:01	bbtest7c	mess...	bbtest7a cron[7596]: (root) MAIL (mailed 63 bytes of output but got status 0
	08.06.2017, 01:40:01	bbtest7c	mess...	bbtest7a cron[7596]: pam_unix(cron:session): session closed for user root

6.1.2 Configuration

The tab 'Query' of the log file display object allows to specify the criteria according to which the log file entries should be displayed. The tab 'Fields' allows to set the fields to be readout in the table. For more information about how to configure the query and the fields:

See also '6.5 | Query' on page 89.

The criteria for querying log files and fields is freely customizable.

A click on the magnifier icon 'Show filter' opens search fields above every table column. Thus, the table entries can be searched by keywords. The search terms found will be highlighted in the table in red. Clicking the arrows left to the search fields allows to switch to the next or to the previous search result. For columns containing dates or times, the filter feature works as follows: When specifying a day, for instance '1.', all data related to the first of a month will be searched. When specifying a day and a month, for example '1.1.', all data related to the 1. January of

the current year will be searched. When specifying a time, only data of the current day containing this time will be searched.

A click on the circle icon left to the search fields filters the log file entries. Only those entries will be displayed that match the search criteria.

Ticking the checkbox 'Reverse order' in the tab 'Data' shows the latest log file entries on top of the table.

A high number of log file entries will be split on several pages. Turn the pages by clicking on the arrows left below the table. Alternatively, use the arrow keys or the page up and page down keys.

6.1.3 Export log information

To export data from a log file, create a log file display object that specifies the criteria according to which the log information should be exported. The table containing the desired information can be exported by clicking on the grid icon right above it. This prompts a pull-down menu offering different file formats for export. The tables can be exported as .xlsx files, .csv files or as lists.

6.2 Updates

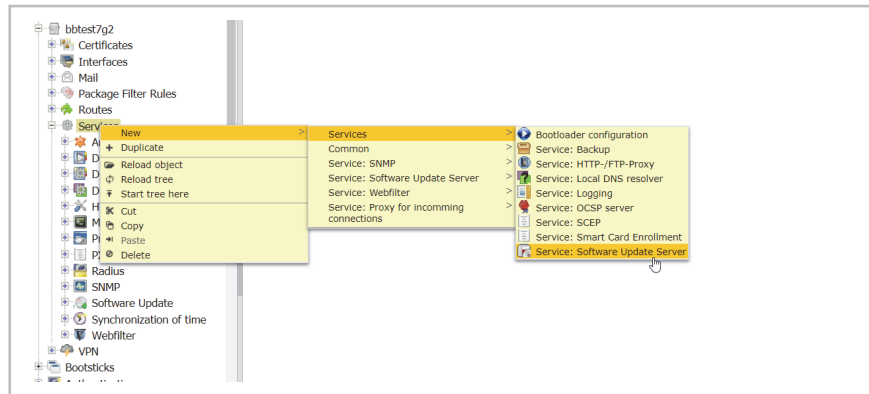
6.2.1 Local update server vs ECOS update server

Updates can be uploaded on ECOS SECURE BOOT STICK in two different ways: through a local update server or through ECOS update server. The update through the ECOS server is directly performed via internet and requires an HTTPS connection to the ECOS update server.

Alternatively, updates can also be made internally with ECOS SYSTEM MANAGEMENT APPLIANCE. In this case, the update is made via the existing master-slave connection. In this way, it is possible to operate boot sticks in different versions as the central management controls the update extent of the different sticks. Thus, the administrator has full control over boot stick updates.

6.3 How to configure updates servers

The service 'Software Update Server' is required for the setup of a local update server. It can be found in the container 'Services' in the ECOS SYSTEM MANAGEMENT APPLIANCE. If the service doesn't exist, it can be created.



If the connection used for updates should not use the regular master-slave tunnel, it is possible to configure an additional connection in the fields 'HTTPS server address' and 'HTTPS server port'.

The field 'Default for Updates' allows to specify a default software source that will be valid for all boot sticks unless another source has been configured on the boot stick under the service 'Software Update'. See also '6.3.3 | Updates for SBS' on page 83.

Tick the box 'Start' to activate the update server.

6.3.1 How to provide images for update servers

In the case of a local update server, it is necessary to provide software update images. To do so, create the configuration object 'Software Update Image' under 'New' > 'Software Update'. Specify its name and click on 'Apply'. You can now upload an image file in the field 'Image'

General Admin	
Name	Version X.XX
Description	
Version	Image Creation Date
Image	Upload
Type	

It is also necessary to create a configuration object of the type 'Software Update Source' in which the software update image will be referenced as the source for the boot stick or the appliance.

General Admin	
Name	Software Update Source
Description	
Source for Secure Boot Stick	Intermediate Version Secure Boot Stick
Source for Appliance	
Source for Installer	
Source for VGA20 Intel	Source for VGA20 ARM
Allow Downgrade	Disable filesystem conversion

This source object can then be referenced on the local update server object in the field 'Default for Updates'.

General Admin	
Name	Software Update Server
Start	<input checked="" type="checkbox"/>
Description	
HTTPS server address	HTTPS server port
Default for Updates	Software Update Source

6.3.2 How to update the appliance

The service 'Software Update' will be required to update the appliance. It should be created in the container 'Services' below the appliance object.

Specify the source for the update in the field 'Software update source'. The source can be either an update server or a software update source object.

6.3.3 Updates for SBS

To always keep ECOS SECURE BOOT STICK up to date, it's recommended to create the service 'Software update' below the boot stick object in the container 'Services'.

The screenshot shows the 'General' configuration tab for a service named 'Software Update'. The interface includes the following fields and options:

- Name:** Software Update
- Description:** (empty text field)
- Software update source:** ECOS Software Update Server (via Internet) (dropdown menu)
- Alternative server address:** (empty text field)
- Check for updates on connection to master:** ☒ (checked)
- Don't check more often than:** 86400 Sec (text field)
- Mode:** ☐ Update ☒ Check only
- Execute at:** Minute [0-59] Hour [0-23] Day [0-31] Month [1-12] WeDay [0-6]
- Use HTTPS proxy:** ☐ (unchecked)
- Proxy address:** (empty text field)
- Proxy port:** (empty text field)
- Proxy user:** (empty text field)
- Proxy password:** (empty text field)

Specify the source for the update in the field 'Software update source'. The source can be either an update server or a software update source object.

If the checkbox 'Check for update on connection to master' has been ticked, the boot stick will automatically check for updates on every connection to the master. This setting is recommended for boot sticks because they are not continually in use, which makes time-controlled updates almost impossible.

The field 'Mode' allows to configure whether the boot stick should only check for new updates or also install them directly.

The field 'Execute at' allows to specify a particular time at which automatic update checks should be performed. The update will then be automatically installed.

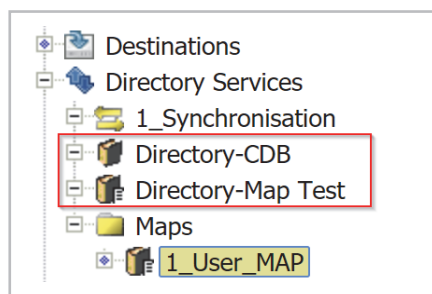
Instead of using the management connection for updating, it is also possible to use the option 'HTTPS Proxy' for a communication via HTTPS proxy. The proxy can be configured in the submenu. If this option is deactivated, a direct HTTPS connection to the internet is required to perform updates.

6.4 Directory synchronization

The directory synchronization allows to import or export objects into/from a directory service, for example to create boot sticks for all users who belong to a particular group in Active Directory (AD). The three configuration objects 'Directory service', 'Mapping' and 'Directory synchronization' will be required for this.

6.4.1 Directory service

Two configuration objects of the type 'Directory service' are required. One is needed to configure the source, the other to configure the destination of the directory synchronization.



The field 'Type' specifies the type of the directory. Following values are available:

- ECOS System: the ECOS SYSTEM MANAGEMENT APPLIANCE itself
- LDAP: any LDAP server
- Microsoft ADS: Microsoft Active Directory
- File

The respective selection opens a submenu that allows to make the settings according to the type.

The screenshot shows the 'General' configuration tab for a directory system. It includes input fields for 'Name' (Directory-CDB) and 'Description'. A 'Type' dropdown menu is set to 'ECOS System'. Below it, 'Resolve pointers' is also set to 'ECOS System'. The 'Allowed operations' section lists 'LDAP', 'Microsoft ADS', and 'File'. Each operation has a corresponding checkbox: 'Change' (checked), 'Add' (checked), 'Remove' (checked), and 'Rename/move' (checked). At the bottom of the form, there are 'Apply' and 'Actions' buttons.

The field 'Allowed operations' controls following read and write permissions:

- Change: objects can be modified
- Add: the directory synchronization can add new objects
- Remove: the directory synchronization can delete existing objects if they are no longer needed in the root directory.
- Rename/move: The directory synchronization can move and rename existing objects.

The tab 'Searchrequest' provides further search options for the synchronized objects.

The field 'Search base DN' specifies the base under which the objects to be synchronized can be searched for the report. This field requires a full DN. If it's left empty, the whole directory will be searched. The destination 'Directory service object' in the field 'Search base DN' determines the container in which to create the new objects.

The option 'LDAP' allows to mention an LDAP search filter and thus to restrict the source objects to a group for example.

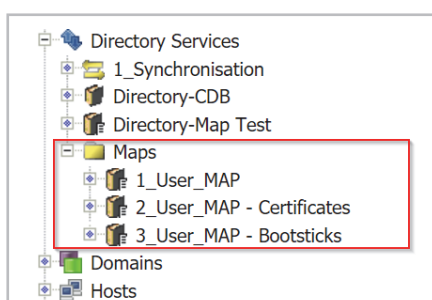
6.4.2 Directory map

The object 'Directory map' allows to create a list in which source attributes can be assigned to their respective destination attributes. The field 'Source object class' defines the object class to which the mapping will be applied. The field 'Destination object class' specifies which object class should be used when creating new objects.

The ECOS system provides some preconfigured default mappings. The field 'Generate default map' and a click on 'Apply' displays the options available. All other fields will then be overridden. The preconfigured fields can be customized afterwards.

Active	Single valued	Source attribute	Destination attribute	Expression on source	Rewrite destination
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	cn	cn		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	sn cn	sn		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	samAccountName	uid		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	c			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	telephonenumber	telephone_number		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	description			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	wwwhomepage	labeled_uri		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	mail			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	proxyAddresses	proxy_addresses		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	givenName	given_name		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	streetAddress	street_address		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	o	ebos_company		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	postOfficeBox	post_office_box		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	facsimiletelephonenumber	facsimile_telephone_number		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	mobile			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	displayName	display_name		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	roomNumber	room_number		

It's possible to create several Directory map objects in one container to define the mapping of single object classes. In the object 'Directory synchronization' the container can then be handed over as map. It is thus possible to create several destination objects (for example a user and a boot stick) from one source object.



6.4.3 Directory synchronization

It is necessary to specify source, destination and a mapping between the two directories in the configuration object 'Directory synchronization'.

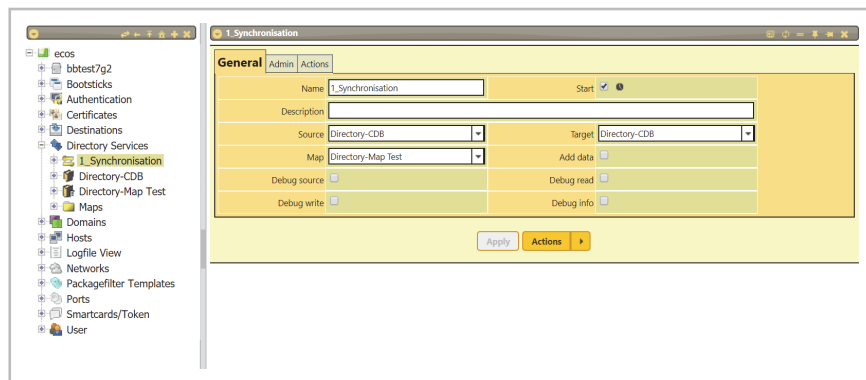
Ticking the checkbox 'Start' activates the automatic directory synchronization. The container 'Directory services' determines when the synchronization will be performed. A manual directory synchronization can be performed regardless whether the object has been activated or not.

The fields 'Source' and 'Target' determine the provider that will make available the source data, respectively the provider through which the data will be written into the destination directory.

The field 'Map' references the directory map object that specifies the attributes to be synchronized and how they should be assigned to each other. It is also possible to select a container with several mapping objects. In this case, the suitable mapping will be determined in the mapping object by the source class, respectively various destination objects will be created when different source object classes coincide.

When the checkbox "Add data" is ticked, new data can be added to existing objects, but no objects created nor existing objects deleted. This setting is only recommendable when several directory synchronizations have been set to write onto the same destination object. This option shouldn't be activated on a regular basis.

The action 'Start Synchronization Manually' directly starts the directory synchronization, regardless whether the checkbox 'Start' has been ticked or not.



6.5 Query

The query object allows to create and manage summary tables of other configuration objects. The table possesses all properties and features explained in the chapter '2.6.4 | Tables' on page 27.

The form of the query object contains the tabs 'General', 'Query', 'Fields' and 'Highlight'.

6.5.1 Tab 'General'

The tab 'General' specifies the name of the configuration object and, if desired, its description. It also displays the summary table, which can be configured in the other tabs.

General							
Query Fields Highlight Chart Admin							
Name Certificate							
Description							
33 Rows all auto 25 50 100 Result							
*		Name	Type of Object	Subject	Valid to	Issuer	Modified
		SSLVPN Rout...	X-509 server certifi...	cn=SSLVPN Router h...	21.04.2022, 04:29	cn=VPN CA,ou=Zertif...	22.09.2017, 06:10
		SSL VPN De...	X-509 server certifi...	cn=SSLVPN Demo Se...		cn=CA ECOS Demo,o...	22.09.2017, 06:10
		X-509 Server...	X-509 server certifi...	CN=x-509 server-zert...	26.04.2016, 09:02	CN=ca-zertifikat,OU=...	22.09.2017, 06:10
		master-rz	X-509 server certifi...	cn=master-rz,ou=Zer...	12.03.2017, 13:46	cn=CA-ecos,ou=Zertif...	22.09.2017, 06:10
		10.14.11.2	X-509 server certifi...	cn=10.14.11.2,ou=Z...	08.01.2016, 13:43	cn=10.14.11.2,ou=Z...	22.09.2017, 06:10
		10.11.11.4	X-509 server certifi...	cn=10.11.11.4,ou=Z...	21.03.2016, 07:22	cn=10.11.11.4,ou=Z...	22.09.2017, 06:10
		SSLVPN Rout...	X-509 server certifi...	cn=SSLVPN Router O...	09.01.2022, 07:59	cn=VPN CA,ou=Zertif...	22.09.2017, 06:10
		Cert SSL VPN...	X-509 server certifi...	cn=Cert SSL VPN Ein...		cn=CA ecos Einwahl...	22.09.2017, 06:10
		SSL VPN Rou...	X-509 server certifi...	cn=SSL VPN Router E...	28.05.2022, 12:14	cn=CA Eschborn User...	22.09.2017, 06:10
		srvvm1.ecos...	X-509 server certifi...	cn=srvvm1.ecos.de,o...	27.05.2014, 12:22	cn=CA ECOS Demo,o...	22.09.2017, 06:10
		hz-gw-2	X-509 server certifi...	cn=hz-gw-2,ou=Zertif...	29.05.2017, 10:10	cn=CA-ecos,ou=Zertif...	22.09.2017, 06:10

6.5.2 Tab 'Query'

6.5.2.1 Selects the document type

The tab 'Query' specifies the document type of the query. After selecting the document type, like shown for the X-509 server certificate, all configuration objects of this type are listed in the table.

General							
Query Fields Highlight Chart Admin							
Type of Object X-509 server certificate Datasource Konfiguration							
Select criteria							
Active/Attribut Comparison Value to Compare Conjunction							
DN =~ ou=CA-DEMO and							
No automatic search							
5 Rows all auto 25 50 100 Result							
*		Name	Type of Object	Subject	Valid to	Issuer	Modified
		demo1.ecos.de	X-509 server certifi...	cn=demo1.ecos.de,o...	16.10.2013, 08:55	cn=CA ECOS Demo,ou=SSLVPN Demo,o...	22.09.2017, 06:10
		IPSec VPN Demo Ser...	X-509 server certifi...	cn=IPSec VPN Demo ...	05.10.2016, 08:50	cn=CA ECOS Demo,ou=SSLVPN Demo,o...	22.09.2017, 06:10
		srvvm1.ecos.de	X-509 server certifi...	cn=srvvm1.ecos.de,o...	27.05.2014, 12:22	cn=CA ECOS Demo,ou=SSLVPN Demo,o...	22.09.2017, 06:10
		SSL VPN Demo Client	X-509 server certifi...	cn=SSLVPN Demo CL...		cn=CA ECOS Demo,ou=SSLVPN Demo,o...	22.09.2017, 06:10
		SSL VPN Demo Server	X-509 server certifi...	cn=SSLVPN Demo Se...		cn=CA ECOS Demo,ou=SSLVPN Demo,o...	22.09.2017, 06:10
5 Rows							
Apply Search Actions							

6.5.2.2 How to create and compare attributes

If only configuration objects with a particular attribute value should be displayed, it can be specified in the tab 'Query'. To do so, click on the arrow in the field 'Attribute' to open the pull-down menu, select the desired attribute, for example 'Valid to', and the value to which you want to compare it.

Possible comparison operators

Comparison operator	Comparison	Explanation
==	equal	
!=	unequal	
>	greater	
<	lesser	
>=	equal or greater	
=	equal or lesser	
=*	Wildcard	Searching for terms containing wildcards ? for exactly one character * for any number of characters (including zero)
!*	no wildcard	Returns all values that don't contain the comparison value (contrary of wildcard)
=~	regular expression	http://perldoc.perl.org/perlre.html#Regular-Expressions
!~	irregular expression	Returns all values that don't contain the regular expression

Table 6.2 Comparison operators

The field 'Value to compare' always adapts to the selected attribute. In the case of a date, for instance 'Valid to', a calendar mask allows to select the comparison value (the date can also be inserted manually).

If 'CA' is selected, clicking on the arrow in the field 'Value to compare' will open a pull-down menu with the relevant options.

The screenshot shows the 'Query' tab in the interface. The 'Type of Object' is set to 'X-509 server certificate' and the 'Datasource' is 'Konfiguration'. Under 'Select criteria', there are two rows: 'DN' with comparison '≈~' and value 'ou=demo', and 'Valid to' with comparison '≈=' and value '31.12.2020'. A date selection calendar is open, showing the month of July 2020. The calendar has a 'Today' button and a 'Done' button.

A date field also allows to enter an expression like 'd+30'. 'D' means day and '+30' specifies the number of days, so 30 days after today. It is also possible to use 'm' for the month and 'y' for the year. In case of a past date, use '-' instead of '+'. Thus, queries rely on the current date. Example: Which certificate expires in the next 30 days?

The following example lists only X-509 server certificates expiring before the 31.12.2020 and whose CA is the 'ECOS Demo CA'.

The screenshot shows the 'Query' tab with the same criteria as before, but the 'Value to Compare' for 'Valid to' is now '31.12.2020'. Below the criteria, there is a table with 4 rows of results. The table has columns: Name, Type of Object, Subject, Valid to, Issuer, and Modified. The results are as follows:

Name	Type of Object	Subject	Valid to	Issuer	Modified
srvvm1.ecos.de	X-509 server certific...	cn=srvvm1.ecos.de,o...	27.05.2014, 12:22	cn=CA ECOS Demo,o...	22.09.2017, 06:10
demo1.ecos.de	X-509 server certific...	cn=demo1.ecos.de,o...	16.10.2013, 08:55	cn=CA ECOS Demo,o...	22.09.2017, 06:10
IPSec VPN Demo Ser...	X-509 server certific...	cn=IPSec VPN Demo ...	05.10.2016, 08:50	cn=CA ECOS Demo,o...	22.09.2017, 06:10
test_1	X-509 server certific...	CN=test_1,OU=CA-D...	09.03.2019, 16:34	CN=test_1,OU=CA-D...	09.03.2018, 16:34

At the bottom of the table, there are buttons for 'Apply', 'Search', and 'Actions'.

The icons and in the toolbar of the select criteria allow to add or remove further comparisons. To remove a comparison, click on it first to tag it.

Modifications will only be shown once the comparison has been activated by ticking it's checkbox in the column 'Active' and the modifications confirmed by clicking on 'Apply'.

6.5.2.3 Disabling automatic search

Normally, the query table is automatically loaded when the query is opened and every time parameters of the query are changed and confirmed with 'Apply'. To deactivate this, tick the checkbox 'No automatic search'.

A click on the button 'Search' at the bottom of the form reloads the table manually.

Active	Attribut	Comparison	Value to Compare	Conjunction
<input checked="" type="checkbox"/>	DN	≈ ~	ou=demo	and
<input checked="" type="checkbox"/>	Valid to	<=	31.12.2020	and

No automatic search ☒

Apply Search Actions

6.5.3 Tab 'Fields'

The tab 'Fields' specifies which properties of the listed configuration objects should be displayed in the table. The field 'Source of field lists' offers the options 'Standard', 'Define' and 'From other query'. The option 'Standard' shows the pre-defined attributes that are suitable for the configuration object.

6.5.3.1 Defining fields manually

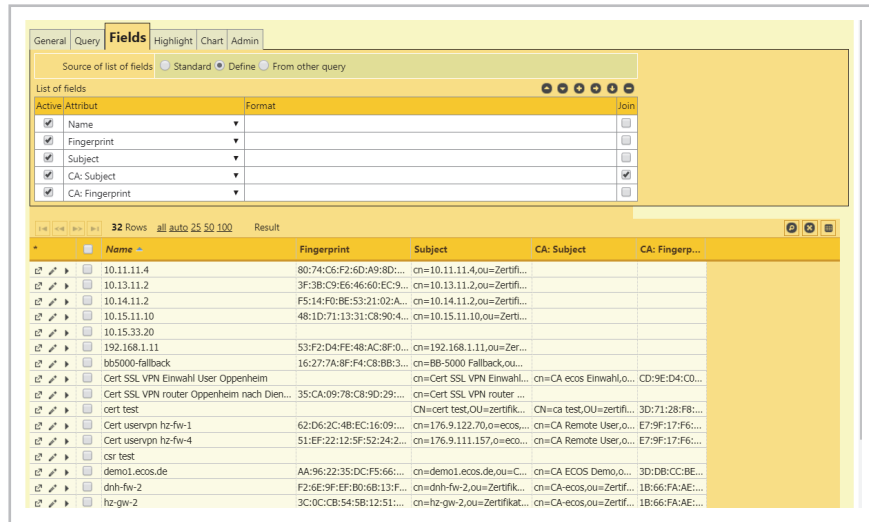
The field 'Define' allows to freely select the desired fields from the attributes of the respective configuration objects.

Select the relevant attribute from the field list that appears when clicking on the arrow in the field 'Attribute'.

Tick the checkbox 'Active' to activate the modification and apply (by clicking either on the icon ☒ in the bar of the configuration object or on the 'Apply' button below the form).

To add or delete further fields use the icons  and  in the toolbar of the field list.

The field order can be customized with the arrows  and .



Name	Fingerprint	Subject	CA: Subject	CA: Fingerprint
10.11.11.4	80:74:C6:F2:6D:A9:8D:...	cn=10.11.11.4,ou=Zertifi...		
10.13.11.2	3F:3B:C9:E6:46:60:EC:9...	cn=10.13.11.2,ou=Zertifi...		
10.14.11.2	F5:14:F0:BE:53:21:02:A...	cn=10.14.11.2,ou=Zertifi...		
10.15.11.10	48:1D:71:13:31:C8:90:4...	cn=10.15.11.10,ou=Zerti...		
10.15.33.20				
192.168.1.11	53:F2:D4:FE:48:AC:8F:0...	cn=192.168.1.11,ou=Zer...		
bb5000-fallback	16:27:7A:8F:F4:C8:BB:3...	cn=BB-5000 Fallback,ou=...		
Cert SSL VPN Einwahl User Oppenheim		cn=Cert SSL VPN Einwahl...	cn=CA ecos Einwahl,o...	CD:9E:D4:CD:...
Cert SSL VPN router Oppenheim nach Dien...	35:CA:09:78:C8:9D:29:...	cn=Cert SSL VPN router ...	cn=ca test,OU=zertif...	3D:71:28:F8:...
cert test		CN=cert test,OU=zertif...	cn=CA test,OU=zertif...	3D:71:28:F8:...
Cert uservpn hz-fw-1	62:D6:2C:4B:EC:16:09:...	cn=176.9.122.70,ou=ecos...	cn=CA Remote User,o...	E7:9F:17:F6:...
Cert uservpn hz-fw-4	51:EF:22:12:5F:52:24:2...	cn=176.9.111.157,ou=eco...	cn=CA Remote User,o...	E7:9F:17:F6:...
csr test				
demo1.ecos.de	AA:96:22:35:DC:F5:66:...	cn=demo1.ecos.de,ou=C...	cn=CA ECOS Demo,o...	3D:DB:CC:BE:...
dnh-fw-2	F2:6E:9F:EF:80:6B:13:F...	cn=dnh-fw-2,ou=Zertif...	cn=CA-ecos,ou=Zertif...	1B:66:FA:AE:...
hz-gw-2	3C:0C:CB:54:5B:12:51:...	cn=hz-gw-2,ou=Zertif...	cn=CA-ecos,ou=Zertif...	1B:66:FA:AE:...

Apart from document type attributes it is also possible to select some additional fields of related objects as columns for the table. For example, the document type 'Certificate' offers the attribute fields 'Fingerprint' and 'Subject' of the configuration object 'CA'.

When including fields related to other configuration objects, their attributes can optionally be displayed in the table too by ticking the checkbox 'Join'. The attributes of the related configuration object will then be shown in the pull-down menu. In this example, we included the field 'CA' and ticked 'Join'. The attributes of CA are prefixed by 'CA ->' in the pull-down menu of attributes.

The additional attributes will also be listed in the selection function of the tab 'Query'.

Active	Attribut	Format	Join
<input checked="" type="checkbox"/>	Name		
<input checked="" type="checkbox"/>	Fingerprint		
<input checked="" type="checkbox"/>	Subject		
<input checked="" type="checkbox"/>	CA: Subject		
<input checked="" type="checkbox"/>	CA: Fingerprint		

	Name	Fingerprint	Subject	CA: Subject	CA: Fingerprint
10.11.11.4	10.11.11.4	80:74:C6:F2:6D:A9:8D...	cn=10.11.11.4,ou=Zertif...		
10.13.11.2	10.13.11.2	3F:3B:C9:E6:46:60:EC:9...	cn=10.13.11.2,ou=Zertif...		
10.14.11.2	10.14.11.2	F5:14:F0:BE:53:21:02:A...	cn=10.14.11.2,ou=Zertif...		
10.15.11.10	10.15.11.10	48:1D:71:13:31:C8:90:4...	cn=10.15.11.10,ou=Zertif...		
10.15.33.20	10.15.33.20				
192.168.1.11	192.168.1.11	53:F2:D4:FE:48:AC:8F:0...	cn=192.168.1.11,ou=Zer...		
bb5000-fallback	bb5000-fallback	16:27:7A:8F:F4:C8:BB:3...	cn=BB-5000 Fallback,ou...		
Cert SSL VPN Einwahl User Oppenheim	Cert SSL VPN Einwahl User Oppenheim		cn=Cert SSL VPN Einwahl...	cn=CA ecos Einwahl,ou...	CD:9E:D4:C0...
Cert SSL VPN router Oppenheim nach Dien...	Cert SSL VPN router Oppenheim nach Dien...	35:CA:09:78:C8:9D:29:...	cn=Cert SSL VPN router ...		
cert test	cert test		CN=cert test,OU=Zertif...	CN=ca test,OU=Zertif...	3D:71:28:F8:...
Cert usvpn hz-fw-1	Cert usvpn hz-fw-1	62:D6:2C:4B:EC:16:09:...	cn=176.9.122.70,ou=ecos...	cn=CA Remote User,o...	E7:9F:17:F6:...
Cert usvpn hz-fw-4	Cert usvpn hz-fw-4	51:EF:22:12:5F:52:24:2...	cn=176.9.111.157,ou=eco...	cn=CA Remote User,o...	E7:9F:17:F6:...
csr test	csr test				
demo1.ecos.de	demo1.ecos.de	AA:96:22:35:DC:F5:66:...	cn=demo1.ecos.de,ou=C...	cn=CA ECOS Demo,o...	3D:DB:CC:BE...
dnh-fw-2	dnh-fw-2	F2:6E:9F:EF:B0:6B:13:F...	cn=dnh-fw-2,ou=Zertif...	cn=CA ecos,ou=Zertif...	1B:66:FA:AE...
hz-qw-2	hz-qw-2	3C:0C:CB:54:5B:12:51:...	cn=hz-qw-2,ou=Zertif...	cn=CA ecos,ou=Zertif...	1B:66:FA:AE...

The field 'Format' of the field list allows to customize the view of the table fields. The expression 'text = xy' renames the title of the corresponding column 'xy'.

Active	Attribut	Format	Join
<input checked="" type="checkbox"/>	Name	text=certificatename	
<input checked="" type="checkbox"/>	Fingerprint	text=fingerprint	
<input checked="" type="checkbox"/>	Subject	text=different subject	
<input checked="" type="checkbox"/>	CA: Subject		
<input checked="" type="checkbox"/>	CA: Fingerprint		

	certificaten...	fingerprint	different subject	CA: Subject	CA: Fingerprint
srvvm1.ecos...	B0:1E:01:FA:...	cn=srvvm1.ecos.de,o...	cn=CA ECOS ...	3D:DB:CC:BE...	
demo1.ecos.de	AA:96:22:35:...	cn=demo1.ecos.de,o...	cn=CA ECOS ...	3D:DB:CC:BE...	
IPSec VPN D...	C1:94:CD:4F:...	cn=IPSec VPN Demo ...	cn=CA ECOS ...	3D:DB:CC:BE...	
test_1	AF:B5:7D:D6:...	CN=test_1,OU=CA-D...			

6.5.4 Highlights

Configuration objects can be highlighted in the table by color according to the same principle as for the selection feature in the tab 'Query'. Select the color (options are red, yellow, green and blue) you wish to use to highlight a particular object, activate it by ticking the checkbox 'Active' and then click on 'Apply'. If a configuration object meets the color highlight criteria, it will be highlighted by the color symbolizing the highest priority. The priorities are in descending order: red, yellow, green, blue.

The screenshot displays the 'Highlight' configuration window. It includes tabs for 'General', 'Query', 'Fields', 'Highlight', 'Chart', and 'Admin'. The 'Highlight' tab is active, showing a 'Source of highlighting' section with 'Define' selected. Below this, there are four sections for highlighting by color: red, yellow, green, and blue. Each section has a 'Valid to' checkbox, a 'Comparison' dropdown, a 'Value to Compare' input, and a 'Conjunction' dropdown. The 'Valid to' checkboxes are checked for red, yellow, and green, and unchecked for blue. The 'Comparison' dropdowns are set to '<=' for red, yellow, and green, and '==' for blue. The 'Value to Compare' inputs are 'd+400' for red, yellow, and green, and 'd+400' for blue. The 'Conjunction' dropdowns are set to 'and' for red, yellow, and green, and 'or' for blue.

Below the configuration settings is a table with 32 rows. The table has columns for 'certificatename', 'fingerprint', 'different subject', 'CA: Subject', and 'CA: Fingerprint'. The table shows various certificates and their associated fingerprints and subjects. The first few rows are highlighted in red, yellow, green, and blue, corresponding to the highlighting settings.

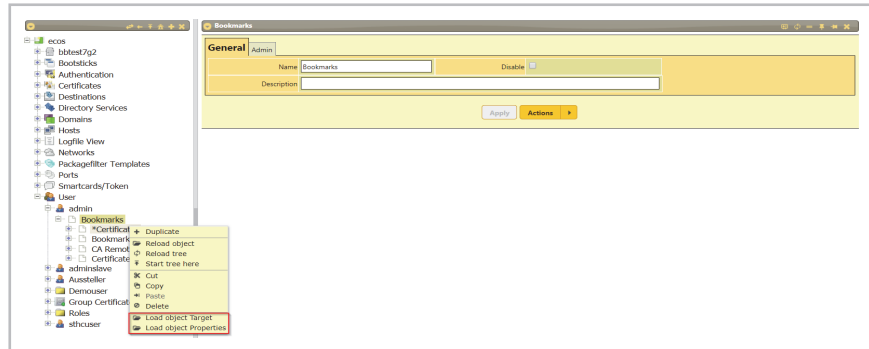
6.6 Bookmarks

Bookmarks allow a quick access to configuration objects or whole page layouts.

Bookmarks are stored separately for each user. Below every user in the tree is a folder named 'Bookmarks' that contains the stored bookmarks. Selecting a bookmark opens the correspondent configuration object or a page with several configuration objects referring to the bookmark.

A right-click on a bookmark opens a pull-down menu. For an explanation of the different options: See also '2.4.2 | Context menu' on page 13.

For 'Bookmarks', the menu is extended by the options 'Load Document Target' and 'Load Document Properties'. The option 'Load Document Target' opens the configuration object or configuration objects referenced by the bookmark. The option 'Load Document Properties' opens the bookmark form in which the bookmark in question can be customized (for example to modify the name or owner of the bookmark).



To delete a bookmark, right-click on it in the tree and select 'Delete' in the menu.

For more information about creating bookmarks See also '2.5.2 | Bookmarks' on page 18. and calling bookmarks. '2.6.2 | Menu bar of the configuration object' on page 23

6.7 Permissions

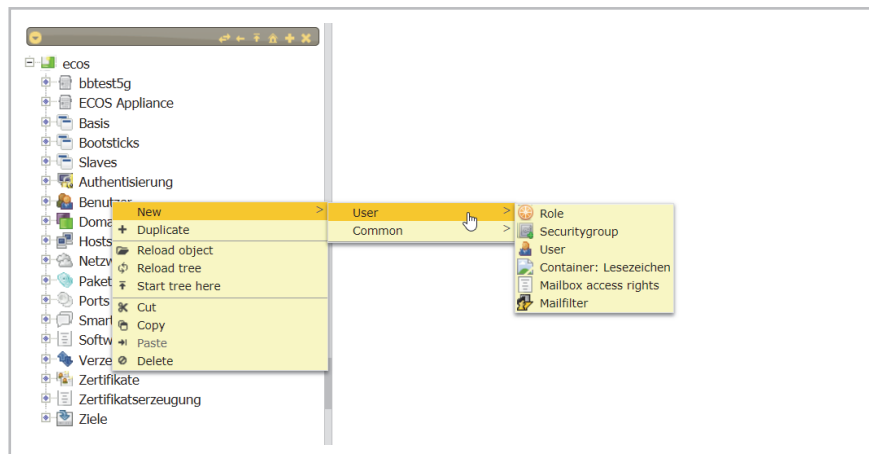
It is possible to assign different permissions to different users and thus define to which configuration objects users have access. Single users can be given an administrator access in the tab 'General' of the respective user form. As administrator, this user will be authorized to access, modify or delete all configuration objects and features.

A user can be given only a restricted access by assigning him a role. Roles can be created individually and associated with specific permissions.

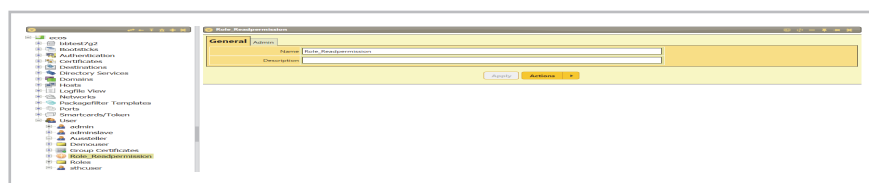
Tick the checkbox 'Access to admin interface' to allow a user to log into the administrator interface. The further role assignment will determine what kind of objects this user will be able to see or modify.

6.7.1 How to create roles

To create a new role, right-click on the folder 'User' and then 'New'> 'User'> 'Role'.



A form appears in which to specify a name and a description of the role. A click on 'Apply' stores the role and displays it in the tree in the folder 'User'.



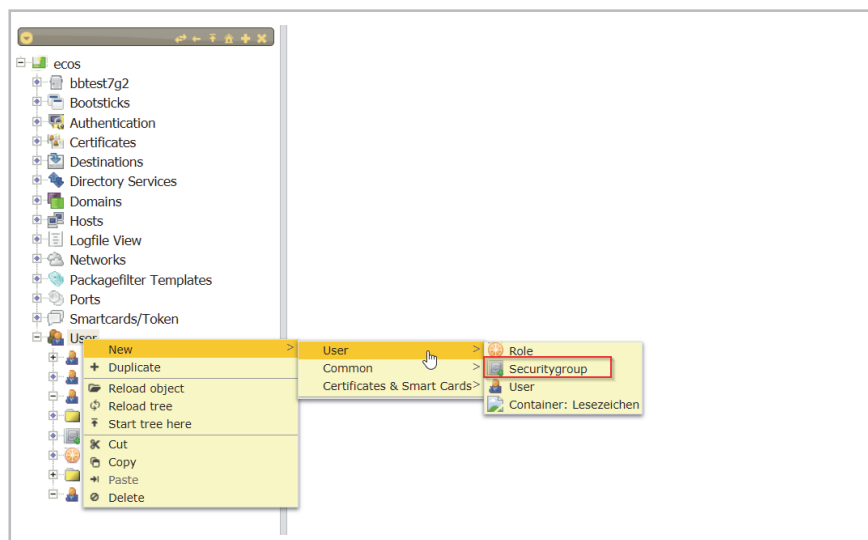
6.7.2 How to assign roles to users

Already created roles can be assigned to users in their respective form in the tab 'General'. Clicking on the arrow next to the selection box 'Role' opens a pull-down menu that contains all created roles.

Click on one of these roles and then on 'Apply' to assign the user that particular role.

6.7.3 How to group roles

Roles can be grouped into security groups in order to assign them specific permissions. To create a new security group, right-click on the folder 'User' and select 'New' > 'User' > 'Securitygroup'. This opens the form of the security group in which to specify the name and assign the different roles.



A click on the arrow next to the selection box 'Roles' opens a pull-down menu that contains all existing roles. Further roles can be added or removed by using the arrows + -.

Click on 'Apply' to store the group.

6.7.4 How to assign group permissions

To assign a specific permission to a group, use the tab 'Admin' of the configuration object for which you wish to control access. Permissions can only be assigned by users who have an administrator access or are authorized to assign 'Rights' for the object in question.

Select the security group from the table 'Rights' and assign the desired permissions by ticking the relevant checkboxes in the fields 'Browse', 'Read', 'Write', 'Create', 'Delete', 'Secrets', 'Rights', 'Admin', 'Parents' and 'Inherit'.

To activate the permission, tick the checkbox in the column 'Active' on the left of the table and store the modifications by clicking on 'Apply'.

The table 'Effective Rights' shows which permissions a role possesses for the actual object.

General

Admin

ID	b832f4b15473014322da2942b002f117	Type of Object	Role
Created	09.03.2018, 15:46	Created By	admin
Modified	09.03.2018, 15:53	Modified By	admin
State of Object	Error in Object		
Im-/Export	Download Upload	Export with Dependencies	Download
Admin info	Source text References of this object Reference to this object Repair		

Rights

Active

Securitygroup

Apply to

Browse

Read

Write

Create

Delete

Execute

Secrets

Rights

Admin

Parents

Inherit

<input checked="" type="checkbox"/>	Group Certificate		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
-------------------------------------	-------------------	--	-------------------------------------	-------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	-------------------------------------	-------------------------------------

Effective Rights

Securityrole	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
Role Issuer	X	X	-	-	-	-	-	-	-	X	X
Role Distributor	X	X	-	-	-	-	-	-	-	X	X

Apply

Actions

Permissions can also be restricted to particular object types. This is particularly relevant in connection with the right 'Inherit'. In this case, the corresponding setting is only applied to objects of the selected type.

GeneralAdmin

ID	b832f4b15473014322da2942b002f117	Type of Object	Role
Created	09.03.2018, 15:46	Created By	admin
Modified	09.03.2018, 15:54	Modified By	admin
State of Object	Error in Object		
Im-/Export	Download Upload	Export with Dependencies	Download
Admin info	Source text References of this object Reference to this object Repair		

Rights

Active Securitygroup

Apply to

Browse

Read

Write

Create

Delete

Execute

Secrets

Rights

Admin

Parents

Inherit

☒ Group Certificz X-509 server certificate☐☒☐☐☐☐☐☐☐☐☒

Effective Rights

Securityrole	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
	-	-	-	-	-	-	-	-	-	-	-

Apply

Actions

6.7.5 Type of permissions

6.7.5.1 Browse

Users with the right to 'Browse' are able to see the correspondent configuration object in the tree. They will also see it in the search query, but they will not be able to open the form of the configuration object.

6.7.5.2 Read

Users with the right to 'Read' can open the form of the corresponding configuration object, but not modify it.

6.7.5.3 Write

Users with the right to 'Write' can open and modify the form of the corresponding configuration object.

6.7.5.4 Create

Users with the right to 'Create' can create new configuration objects of the same type.

6.7.5.5 Delete

Users with the right to 'Delete' can remove configuration objects of the corresponding type.

6.7.5.6 Secrets

Users with the right 'Secrets' have access to authentication data such as passwords.

6.7.5.7 Rights

Users with the right 'Rights' can assign permissions to other users.

6.7.5.8 Admin

Users with the right 'Admin' have access to the object administration. They can, for instance, display the source text and repair objects.

6.7.5.9 Parents

When the checkbox 'Parents' is ticked, all configuration objects above the correspondent object in the tree have automatically the right to browse in order to allow the user to navigate to the authorized object.

6.7.5.10 Inherit

When the checkbox 'Inherit' is ticked, the assigned permissions are automatically extended to configuration objects located below the corresponding object in the tree. The permissions can be customized in the tab 'Admin' of the subordinated objects.

6.7.6 Special permission cases

6.7.6.1 One role assigned to several groups

A role can be assigned to several security groups simultaneously. If this is the case, the permissions of both groups are additive, which means that if both security groups have different rights for the same objects, the user will receive the permissions of both groups.

Example: Securitygroup 1 has the right to read and write for the object. Securitygroup 2 has the right to read and delete for the same object. A user whose role has been assigned to both security groups will consequently have the right to read, write and delete for this object.

The screenshot shows the 'Admin' tab for an object. The object details include:

- ID: cd6b6e305787d07307d3344878a6d46f
- Type of Object: Container: Users
- Created: 13.03.2012, 13:45
- Created By: cn=system,dc=ecos,dc=de
- Modified: 09.03.2018, 15:57
- Modified By: admin
- State of Object:
- Error in Object:
- Im-/Export: Download Upload
- Export with Dependencies: Download
- Admin info: [Source text](#) [References of this object](#) [Reference to this object](#) [Repair](#)

The 'Rights' section shows a table with columns: Active, Securitygroup, Apply to, Browse, Read, Write, Create, Delete, Execute, Secrets, Rights, Admin, Parents, Inherit. Two security groups are listed:

Active	Securitygroup	Apply to	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
<input checked="" type="checkbox"/>	Group_1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Group_2		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The 'Effective Rights' section shows a table with columns: Securityrole, Browse, Read, Write, Create, Delete, Execute, Secrets, Rights, Admin, Parents, Inherit. Two roles are listed:

Securityrole	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
Role Issuer	X	X	-	-	X	-	-	-	-	-	-
Role Distributor	X	X	X	-	-	-	-	-	-	X	X

Buttons: Apply, Actions

6.7.6.2 Different rights for parents and subordinated objects

If a security group has been assigned the right to 'Inherit' for a particular configuration object, this group will automatically have the assigned rights for all configuration objects located below the object in question in the tree. If the security group has been assigned divergent permissions for a subordinate object, this permission range will override the range of the parent object.

Example: In the container object 'Certificates' the security group 'Group Certificates' has been assigned the rights to browse, read, create and delete. Furthermore, the rights for 'Parents' and 'Inherit' have been activated. The field 'Effective Rights' shows to which roles the permissions have been assigned. In this case, all roles inside the security group 'Group Certificates' possess the permissions enumerated above.

As 'Inherit' is set active, the permissions are also valid for all subordinated objects, in this case all certificates.

Active	Securitygroup	Apply to	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
<input checked="" type="checkbox"/>	Group Certificate		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Securityrole	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
Role Distributor	X	X	-	X	X	-	-	-	-	X	X
Role Issuer	X	X	-	X	X	-	-	-	-	X	X

So, if the group should get more or less privileges for particular objects or containers, this can be customized in the tab 'Admin' of the corresponding object. The privileges of the parent object will be overridden and no longer be valid.

As the present example shows, the security group 'Group Certificates' has only the rights to browse, write, parents and inherit for all objects inside the container 'CA DEMO'. The rights to 'Create' and 'Delete' are no longer active although they have been set in the parent object 'Certificates'.

Active	Securitygroup	Apply to	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
<input checked="" type="checkbox"/>	Group Certificate		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Securityrole	Browse	Read	Write	Create	Delete	Execute	Secrets	Rights	Admin	Parents	Inherit
Role Distributor	X	X	-	-	-	-	-	-	-	X	X
Role Issuer	X	X	-	-	-	-	-	-	-	X	X

7 Technical support

If you have questions about our products, please contact our support.

You can reach us under:

Tel.: +49 (6133) 939-300

E-Mail: support@ecos.de

For troubleshooting, please contact us Mon - Sun 24h.

Support cases are processed Mon - Fri 8.00 - 18.00, excluding statutory holidays.

Please, keep to hand the serial number of your device.

We recommend that you contact your ECOS partner vendor at first. We support our partners in the best possible way to assist you and they are well-acquainted with IT infrastructures.

Please send your hardware test with a brief description and your contact data to hwtest@ecos.de.

Please report security incidents in writing to support@ecos.de Please also join a detailed description and your contact data.

ECOS release.notes keep you up-to-date concerning updates. Sign up for our newsletter on our website in the support section.

A

- Access restrictions 53
- Actions 22
- Administration interface 9
- Appliance 39
- Attribute 91

B

- Basic setup 39
- Bookmarks 96
- Boot loader 68
- Boot stick 59
- Browser 52

C

- CA certificate 55
- Certificates 54
- Citrix 50
- Citrix Desktop 50
- Citrix Web 51
- Comparison operators 91
- Configuration objects 12, 21
- Connection profiles 48
- Context menu 13
- CRL 56

D

- Directory map 86
- Directory service 84
- Directory synchronization 84, 88
- Duplicate 14

E

- Easy Enrollment 63



ECOS SECURE BOOT STICK 59, 77
ECOS System Connector 60
ECOS SYSTEM MANAGEMENT APPLIANCE 60
Enrolment 59
Export 66

F

Fields 93
File export 30
Filters 28

G

Gateway 41
Group 100
Grouping 32

H

Highlights 96
History 19
Host 42
HTTPS 44

I

Interfaces 40
IPsec 68

L

LDAP 86
License 46
Local admin 77
Local user 77
Log files 79
Login 9

M

Maintenance 45

- Manage printer automatically 71
- Management connection 76
- Mass storage 69
- Menu bar 16, 27

N

- Network addresses 42
- Network configuration 40
- Networks 43

P

- Permissions 97, 103
- Personalization 62
- Popups 38
- Ports 43
- Printer 70

Q

- Query 89

R

- Radius 44
- RDP 49
- Refresh 24
- Role 98

S

- Search 18
- Selection box 26
- Software update server 45
- Sorting 31
- Synchronization 16

T

Tables 27

Tree 12

U

Update server 80

V

VMware 52

VPN 66

VPN connection 68

X

X-509 57



ECOS TECHNOLOGY GMBH

Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Telefon: +49 (6133) 939-0
E-Mail: info@ecos.de
Internet: www.ecos.de
