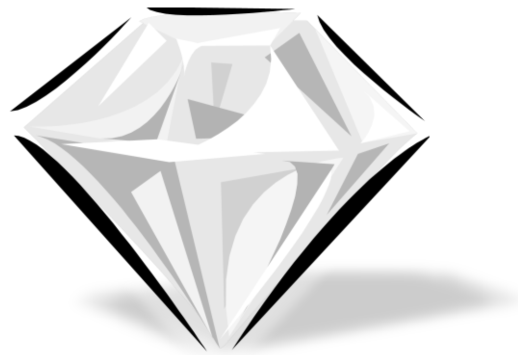
Emerald

Administrator's Guide

Version 6.0.77



Emerald Management Suite

IEA Software, Inc.

SOFTWARE LICENSE AGREEMENT

By purchasing or installing all or part of the Emerald Management Suite, you indicate your acceptance of the following License Agreement.

Ownership of Software -You acknowledge and agree that the computer program(s) and associated documentation contained with the Emerald Management Suite (collectively, the "Software") are owned exclusively by IEA Software, Inc. and/or its licensors. The Software contained in the package is protected under copyright laws and all copyright and other intellectual property rights relating to the Software are and remain the exclusive property of IEA Software, Inc. and/or its licensors. You may not rent or lease the Software, but you may transfer the Software and accompanying materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement.

License - IEA Software, Inc. grants to you, and you accept, a limited, non-exclusive and revocable license to use the Software. You agree to use the Software in machine-readable object code form only as authorized in this License Agreement. This License Agreement does not convey any title or interest in the Software to you. You may only use the licensed number of Master Billing Records (MBRs) with the Software as stated in your purchase agreement.

Scope of License -You may not make any changes or modifications to the Software, and you may not decompile, disassemble, or otherwise reverse engineer the Software. You may not load, rent, lease or sublicense the Software or any copy to others for any purpose. You agree to use reasonable efforts to protect the Software from unauthorized use, modifications, reproduction, distribution and publication. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Agreement, your license will be revoked.

Updates and Support - All software updates are available via the IEA Software, Inc. web site. A maintenance contract is available for major version upgrades, which is not included or covered as part of the basic purchase agreement. Technical support is available via E-Mail, support mailing lists, or a purchased telephone support contract.

Trademarks - IEA Software, Inc., Emerald, RadiusNT, and the associated logo(s) are registered trademarks.

Restricted Rights - The Software is provided with U.S. Governmental Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19 as applicable. The Software is also protected by International Treaty Provisions. Manufacturer is IEA Software, Inc. PO BOX 1170 Veradale WA, 99037

Miscellaneous - This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

Limitations of Liability and Remedies - In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, or the possibility of such damages. IEA Software, Inc. and its licenser’s entire liability and your exclusive remedy shall be, at IEA Software’s option, either

(a) return of price paid, or (b) repair or replacement of the Software. To the maximum extent permitted by applicable law, IEA Software, Inc. and its licensors disclaim all other warranties, either express or implied, including but not limited to, implied warranties with regard to the Software, the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights, which vary from state/jurisdiction to state/jurisdiction.

Should you have any questions concerning this license agreement, please contact IEA Software, Inc. PO BOX 1170 Veradale, WA 99037 U.S.A. (509) 444-BILL (2455).

TABLE OF CONTENTS

PREFACE

Emerald Administrator's Guide is designed to provide detailed technical information for those installing, configuring, and administering Emerald Management Suite. This technical manual complements Emerald User's guide. It is recommended you read material presented within Emerald User's guide prior to attempting to administer Emerald in order to gain a thorough understanding of configuration options available to you.

Emerald Management Suite is designed to utilize Microsoft SQL Server or Oracle relational database package for data storage. The database package must be installed and configured outside of the Emerald Management Suite environment. Emerald documentation offers no specific information regarding the installation, configuration, operation or maintenance of back-end database application. It is highly recommended that the database application documentation be available during Emerald Management Suite installation and setup. A good working knowledge of your database server will aid in understanding some portions of Administrator's Guide.

SYSTEM REQUIREMENTS

Emerald Management Suite operates within a web environment based upon an integrated web server. Emerald is accessed via any standard HTML5/CSS3 compliant browsers. Emerald requires database server access, requiring Microsoft SQL Server to be installed and configured before Emerald installation can be fully completed.

Emerald Management Suite carries following minimum system requirements. Listed requirements are separate from requirements of database server. Please note independent database server installations need only be accessible to the Emerald server and not necessarily reside on the same computer as Emerald software.

- Windows
    - x86 or x64 compatible processor
    - Windows 2000-2022 or XP-11
    - 20 GB free hard disk space for software installation and logs
    - 512 MB available memory for Emerald suite, more recommended
    - SQL Server 2000-2022 (Windows or x64 Linux)
    - HTML5 / CSS3 compatible web browser

- Linux
    - X64 compatible processor
    - Linux x64 kernel 2.6 or later
    - 20 GB free hard disk space for software installation and logs
    - 512 MB of available memory for Emerald suite, more recommended
    - SQL Server 2000-2022 (Windows or x64 Linux)

- HTML5 / CSS3 compatible web browser

INSTALLATION OVERVIEW

Before installing Emerald Management Suite install all necessary Database server components and ODBC drivers on the windows platform. Database connectivity is included on UNIX platforms however Oracle 10+ client access libraries must be installed on UNIX systems if Oracle is to be used. A web browser is required to perform database installation and access Emerald.

> Changes.txt file in Emerald subdirectory notes all recent changes, known problems, platform-specific issues and bug fixes made to Emerald Management Suite. For the latest release and information on Emerald, access https://www.iea-software.com/docs within your web browser.

Installation of Emerald Management Suite itself involves following three steps:

- Installation of Emerald Management Suite
- Creation of Emerald database
- Configuration of Emerald Suite through Emerald Admin options.

As part of the normal installation process your System or Network Administrator will create and populate default data and configuration information for Emerald database. These tasks are outlined within this document. Emerald database must be created and configured before Emerald software can be used.

In the event you experience problems during installation process please contact the IEA Software Customer Support Department for assistance.

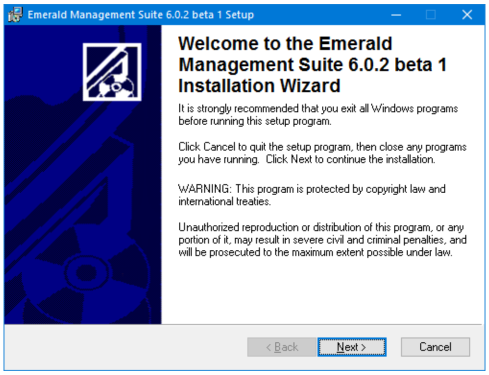
Downloading Emerald from IEA Software Web Site

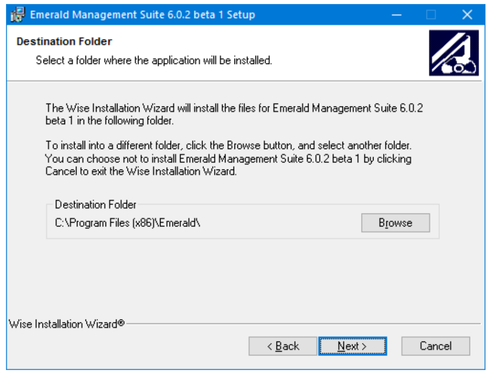
All available product information, documentation, change history and product upgrades for access and/or download are available online from IEA Software main web site. (https://www.iea-software.com/) The site also provides important product information and customer support options for those who encounter problems or have questions through installation or use of Emerald.

Current version of Emerald is available for direct download: https://www.iea-software.com/emerald#download

Windows Installations

Whether installing Emerald v6 for the first time or updating an existing Emerald v6 installation begin by running Emerald6.exe. For added assistance upgrading from versions of Emerald prior to version 6 please see Upgrading from Emerald 5



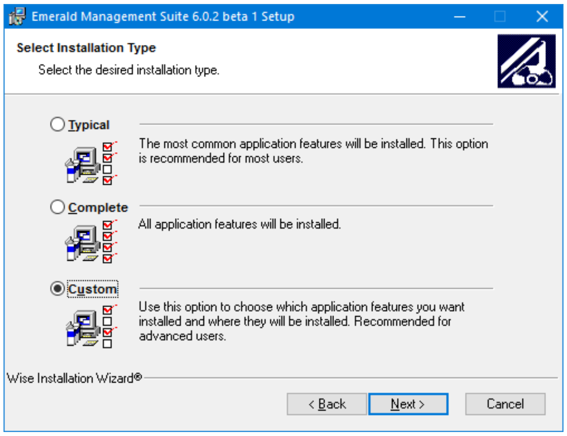


Follow instructions of installation wizard to proceed thru installation process.

If updating an existing installation of Emerald v6 you will be prompted to first remove current version before proceeding. Removal stops all currently running Emerald related services and uninstalls Emerald v6 software yet configuration and custom data stored in Emerald folder is retained. Please consider following when updating Emerald:

- If you have previously installed Emerald v6 into a location other than default please take care to re-enter this location when prompted for destination folder within installation wizard. This ensures items including custom reports and themes remain accessible once update is completed.
- Once installed **RadiusNT** service is configured to startup automatically but **is NOT started automatically**. It can be started from windows services manager or by typing "net start radiusnt" from CLI.
- Emerald Session manager is not started automatically and is configured for manual startup by default. If using Session manager please be sure to set service to start automatically and then start the service using windows services manager.
- All Emerald related services are initially installed using default system account. If running Emerald and related services as a different user account it will be necessary to update "logon as" options in Logon tab of windows services manager for each Emerald related service after installing an Emerald v6 update.
- Once Emerald update has been installed browsing to Emerald web interface may be delayed by several minutes or you may notice a startup message "stage 19: database maintenance update". This delay is normal as database related changes associated with update are automatically synchronized.

Installation features



Selecting typical installation installs following core Emerald Suite Components: Emerald web server, Emerald scheduler, RadiusNT, RadiusNT Admin, RADIUS test client, geoimport and Emerald session manager.

Following optional components require selecting complete or custom installation to install: LDAP Synchronization server, Syslog Server, Emerald Network Collector, SMS Poller and EmerAuth DLL.

Linux Installations

Begin by unarchiving emerald6_linux.tar.gz from within a temporary folder using command:

tar -zxf ./emerald6_linux.tar.gz

Before installing Emerald make sure user is logged on as root user or run installer as the root user.

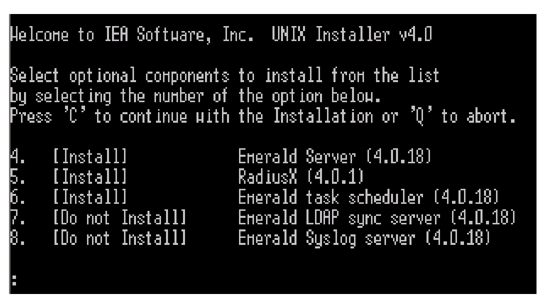
Start Emerald installer by running '**./install.pl**' from temporary folder emerald6_linux.tar.gz was unarchived to.

If you will be updating an existing installation of Emerald v6 please be sure to stop all Emerald related services prior to installation. Updating an existing Emerald v6 installation follows the same installation procedure as initial installation. Existing configuration settings and data including themes and custom reports are preserved when updating an existing installation of Emerald v6.

For added assistance upgrading from versions of Emerald prior to version 6 please see Upgrading from Emerald 5

Installation features

A list of components to be installed is displayed. Features set to be installed appear in the component list with [Install]. To select whether to install or update a feature press the number corresponding with feature selection. When finished making selections press 'C' to continue with product installation.



All Emerald suite components except RadiusX and Air Marshal are installed to the "/usr/local/emerald" folder.

RadiusX and related components are installed to "/usr/local/radius".

Air Marshal is installed to "/usr/local/portal"

Common configuration and database connectivity is managed from "/usr/local/iea"

Initializing and Verifying the Emerald Web Service

During Emerald Management Suite installation Emerald Web Server (Emerweb) service was automatically installed and configured on your system. Emerald Web Server is required to be running in order to access the Emerald Management Suite. The Emerweb Service "Emerald Web Server" is pre-configured to start automatically upon system startup and will be available once the system has been restarted. Emerald must be installed and the Emerald database must be created and configured before Emerald software can be used

By default Emerald Web Server, once installed and initialized will continue to run as a background service without interruption. If necessary Emerald web server can be started in debug mode if not currently running for troubleshooting purposes.

Windows systems:

1. To start the Emerald Web Server, select Web Server Debug Mode from the Start Menu/All Programs/Emerald/Server menu.

Linux systems:

1. To start the Web Configuration Server, change to the /usr/local/emerald directory: "cd /usr/local/emerald".
2. Execute the command "./emerwebsrv –debug 255".

UPGRADING FROM EMERALD 5

This section covers important information covering differences between Emerald v5 and version 6. Before upgrading to Emerald v6 please take some time to read this section carefully. In addition to a significant number of new features the core Emerald system has undergone several major billing related changes. If you are not upgrading from a previous version of Emerald you can skip this section.

Reporting

During upgrade custom reports are not automatically migrated. Emerald version 5 custom reports must be modified for compatibility with Emerald v6 due to database changes.

Web Interface

Emerald browser requirements have changed from HTML4/CSS2 to HTML5/CSS3. Existing custom theme folders designed for Emerald 5 may require minor changes to account for style and UX differences throughout operator and customer interfaces.

Scheduling

No Emerald scheduled tasks are brought over from Emerald v5. Instead a default set of scheduler tasks are installed with new Emerald v6 database. All automatic invoicing, statement creation, CC/EFT batching and emailing of invoices and statements are disabled initially. You may enable these tasks as necessary from the "Emerald Admin" / "Scheduler" / "Configure Schedules" menu.

Notification

- Custom notice types likely require configuration changes to notice query field to remain compatible with Emerald v6 schema changes since version 5.
- Scheduled tasks associated with existing notices are not automatically migrated. Scheduling must be applied from notice Options menu for existing notices post upgrade from Emerald Admin / Messaging / Notices.

Packaged Services

Packages and package types have been replaced with nested services and service categories respectively with following important changes.

- Service categories are mandatory. All services must be associated with a service category
- Once a service is created it can only be changed to other service types within its category
- Every service is able to contribute to account invoice regardless of child/parent relationship
- Parent and child services can be arbitrarily nested as required

During upgrade from Emerald v5 packaged accounts are automatically converted to nested services. For non-packaged services service category conversion utility in Emerald Admin / Services menu can be used to organize existing services into service categories.

RADIUS

- Calls table used to store RADIUS accounting has been replaced with a view for compatibility. Data cannot be deleted or changed from this view.

- NAS-Port no longer required for online session list. It is recommended "Add virtual NAS-Port if missing" RadiusNT/X Advanced menu options or any custom attribute filters that modify or add NAS-Port be disabled.

- Configuration of per-service RADIUS attributes can now be merged rather than strictly replace service type defaults.

- IP pooling features have been replaced by inventory system. Currently static IP addresses can only be assigned to services by operators. Dynamic IP allocation is now managed by Dynamic Addressing option within RADIUS admin menu.

- Some nonstandard attribute labels within Standard attribute space have been renamed to align with standard names. If any custom attribute filters, rating rules or log tables reference these attributes by name references should be updated to maintain compatibility with Emerald v6 otherwise no action is required.

    - NAS-Identifier (ID:4) is renamed NAS-IP-Address
    - User-Service is renamed Service-Type
    - Framed-Address is renamed Framed-IP-Address
    - Framed-Netmask is renamed Framed-IP-Netmask
    - Framed-Filter is renamed Filter-Id
    - Login-Host is renamed Login-IP-Host
    - Callback-Name is renamed Callback-Id
    - NAS-Port-DNIS is renamed Called-Station-Id
    - Caller-ID is renamed Calling-Station-Id
    - Tunnel-Connection is renamed Acct-Tunnel-Connection
    - Signature is renamed Message-Authenticator
    - Sip-Response-Code is replaced with EAP-Key-Name

Billing Related

- Service discounts pay period discounts and service static pricing features have been rolled into Market Tags configured from Emerald Admin / Accounting / Sales & Marketing.

- Emerald introductory offers set using service type level "Next Service Type" & "Next After" are not directly supported. Currently active introductory offers from version 5 are imported as scheduled future service type changes visible from the services timeline. Going forward for new Emerald 6 accounts introductory discounts are implemented using market tag based time limited discounting leveraging "Invoiced Days Max" tag match condition.

- Credits are no longer issued when changing or closing services. Changes affecting term covered by existing invoices are now accounted for by reinvoicing to include relevant account changes.

- Current value of MBR and Service cancel date, cancel reason and service type are ignored and no longer directly affect invoicing. Emerald version 6 invoicing activities are based on configuration of MBR and service timelines. Any custom processes which manually set service type or cancel dates should be modified to call "mbropen", "saopen", "mbrclose", "saclose" and "sachange" exec template functions or change the account timeline.

- When viewing recurring services monthly service cost is only displayed or changed once account has been invoiced. Full invoice processing is required to accurately determine cost. Displayed service cost is informational having no influence on invoicing. Displayed cost is also used by reports including revenue forecast to estimate future invoices.

Signup

- Signup options for services assigned to package are not automatically copied and must be configured manually. One time signup options and recurring signup options where standalone services are provisioned by default are copied.
- "Send Method" and "Customer Pay Options" configuration options have moved from signup option (Formerly package type) to signup server.

Upgrade pre-requisites

When upgrading to Emerald 6 from Emerald 5 you must have the following:

- Separate computer to install the Emerald software different from your current Emerald 5 production system.
- If database server for Emerald v6 will be different from existing version 5 database servers you must first backup and restore Emerald v5 database to the Emerald v6 database server.
- Emerald version 6 license key.
- Emerald v5.0.73 or later must be installed prior to upgrading to Emerald v6.
- Emerald version 2.5 or 4.5 customers wishing to upgrade to Emerald v6 must first upgrade to version 5.

Upgrading Emerald

Upgrade process creates a new database for Emerald 6 copying existing Emerald 5 data into the new database. This process does not alter the source Emerald 5 database but may adversely affect system performance for the duration of the upgrade process.

To upgrade Emerald follow steps outlined in the "Initial Database Configuration" section below. When creating the Emerald 6 database in step 9 choose your existing Emerald 5 database from the "Convert Emerald 5 database" selection list and choose the type and quantity of call records you would like copied into the new Emerald 6 system.

INITIAL DATABASE CONFIGURATION

For new installations of Emerald if you do not have a database server SQL Express edition can be obtained at no cost from the Microsoft website for both Windows and Linux server platforms. SQL Express edition while free for commercial use yet limited to 10 GB per database generally suitable for 20000 active MBRs depending primarily on RADIUS accounting volume and retention period.

https://www.microsoft.com/en-us/sql-server/sql-server-editions-express

https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-setup

Once the Emerald Server installation is complete and the Emerald Web Server has been initialized, the Emerald System Administrator must configure the system. Configuration of the system includes creation and population of Emerald database.

Emerald Administrator must perform following steps, as well as verify independently installed database server and database client access configurations before Emerald Management Suite can be used.

Regardless of operating system platform, each installation requires the initial creation and configuration of the Emerald database performed with the Emerald Web Configuration Server. The steps required to complete the initial configuration of the system are described below.

Start the Emerald Web Configuration Server.

Windows systems:

- To login to the Web Configuration Server, select Web Config from the Start Menu/All Programs/Emerald menu.

Linux systems:

- Open a web browser and go to the URL: http://127.0.0.1/settings

If this is first time that Configuration Server has been started you will initially be prompted to enter a Password and confirm the password value by entering it again. The Web Configuration password entered will only be valid for the Emerald Web Configuration Server (not for Emerald application itself). There is no default username or password when the Web Configuration Server is initially started.

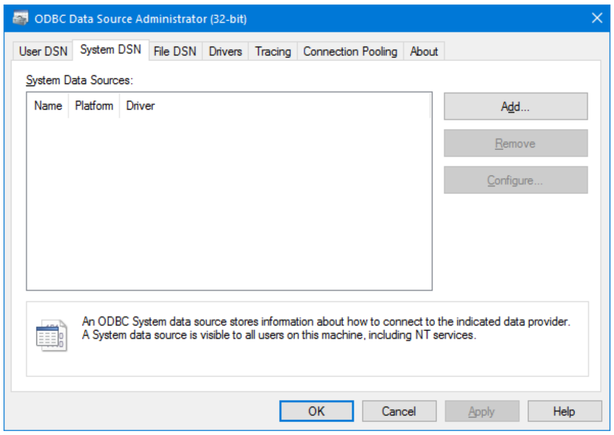
After you have created the Web Configuration Server password, you will be prompted again for a Web Configuration Server username and password to login. The username is insignificant and password is same as initially set for Configuration server above.

Password configured for the Web Configuration Server is shared among all Emerald Management Suite Configuration Server Administrators (Emerald Web Configuration Server, RadiusNT Administrator, RADIUS test client, Air Marshal Administrator, EmerAuth Administrator, etc.), meaning all Administrators running on the same machine will use the same password once it has been established.

```
If Emerald configuration server password is forgotten it can be reset using
following instructions.  Once reset you will be prompted to set a new
password on next access to configuration server.
```

```
Windows:  Use 32-bit Registry Editor to locate "WCPassword" field under
HKEY_LOCAL_MACHINE\Software\IEA\Common.  Delete the entire WCPassword key
within registry editor.  It is important this key be deleted and not simply
set to have no value.

Linux: Use a text editor to remove entire line starting with "WCPassword ="
from file /usr/local/iea/common.ini
```



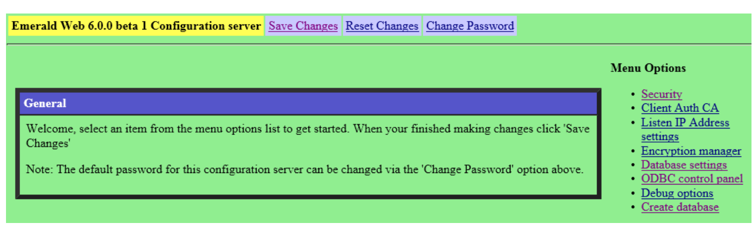
If using Windows it is recommended you first create an ODBC datasource to be used by Emerald to access your database server.

Create a 32-bit "System DSN" from Windows ODBC control panel. A link to control panel is available from Start Menu / All Programs / Emerald / Operating System / ODBC Control Panel (32-bit)

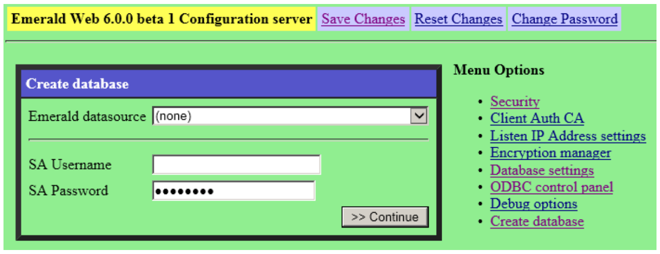
When configuring datasource it is important to make sure datasource name contains only alphanumeric characters and does not contain any spaces or symbols. It is also very important to disable all character translation and make sure a default database to be used by Emerald is set. Please test database access to confirm connectivity before continuing.

```
Windows: There are three different similarly worded SQL Server ODBC drivers
for Windows.  "SQL Server", "SQL Server Native Client xx" and "ODBC Driver xx
for SQL Server".  It is recommended use of legacy "SQL Server" driver be
avoided.  "SQL Server" driver is not updated with support for new database
features and has defects known to interfere with reliable operation of
Emerald.  Any version of "SQL Server Native Client xx" or "ODBC Driver xx for
SQL Server" supported by your database server is fully compatible with
Emerald.  "SQL Native Client xx" has subsequently been superseded by "ODBC
Driver xx for SQL Server".
```

Once Emerald Web Configuration Server has been launched choose "Create Database" Menu option to the right of welcome message. If upgrading from Emerald v5 it is also necessary to create a new database. Your existing data and settings will be migrated into the new database during database creation.

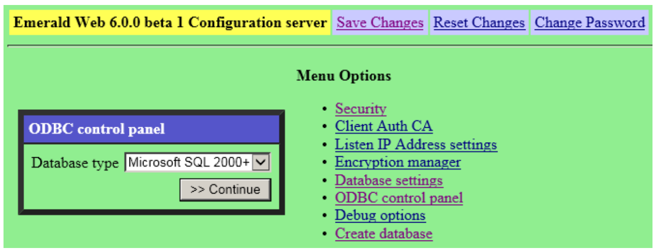


Within the Create Database screen, you are prompted to configure the Emerald data source information to establish ODBC connectivity to your database server. If you have not already created an ODBC datasource you may create one by selecting the ‘New’ option from Emerald datasource pick list and then press the Continue button.

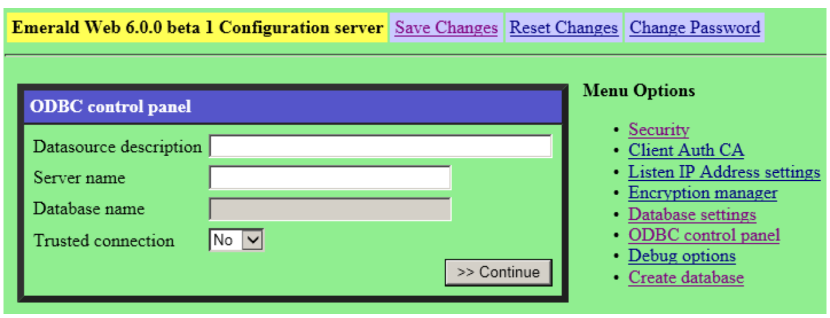


On the ODBC control panel screen, enter "Emerald6" in the Create new datasource field. Alternatively, you may select an existing datasource to edit from the Edit existing datasource pick list.

Choose the appropriate type from the Database type pick list. This indicates the type of database server installed on your site that will run against the Emerald server. Your choice will be a Microsoft SQL or Oracle selection



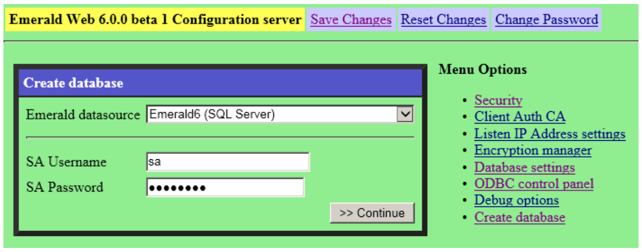
The next step is to describe the new Emerald data source and provide server information. Enter the following information on the fields provided



Field	Description
Datasource description	Enter a description for the datasource. Generally, this will be the datasource name "Emerald6". Description should be alphanumeric only and not contain any spaces or symbols.
Server name	Enter the name of the server in which your database server resides. Note: For UNIX versions the server name is the IP Address of your database server followed by ',' and its TCP port number. Example: 10.0.0.35,1433
Trusted connection	Choose Yes or No from the pick list indicating whether your database server will be accepting a Trusted connection, or using the SA username/password information for Emerald access.

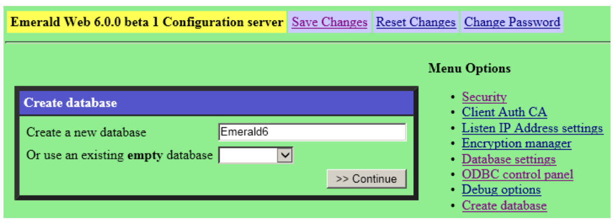
If datasource is not configured to use a trusted connection use an existing account with preexisting database created for use with Emerald or the system administrator (SA) username and password to establish access to the database.

Field	Description
Emerald data source	Choose the Emerald datasource name, typically 'Emerald6', from the data source pick list.
SA Username	Enter the system administrator username configured on your database server.
SA Password	Enter the system administrator password configured on your database server.



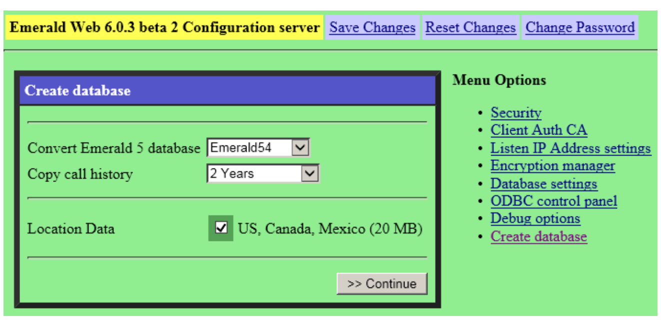
The next step in the database configuration is to create Emerald database that will store all account and system information.

If using SQL Server you may either create a new database using SQL Management Studio or by entering 'Emerald6' as database name in Create a new database field in the create database screen.



If using Oracle please login as a user associated with a tablespace intended to be used by Emerald.

Continuing on with the Create Database task, this screen is used to identify information for your existing database server, and indicate if a data upgrade from a previous Emerald version installation is required.



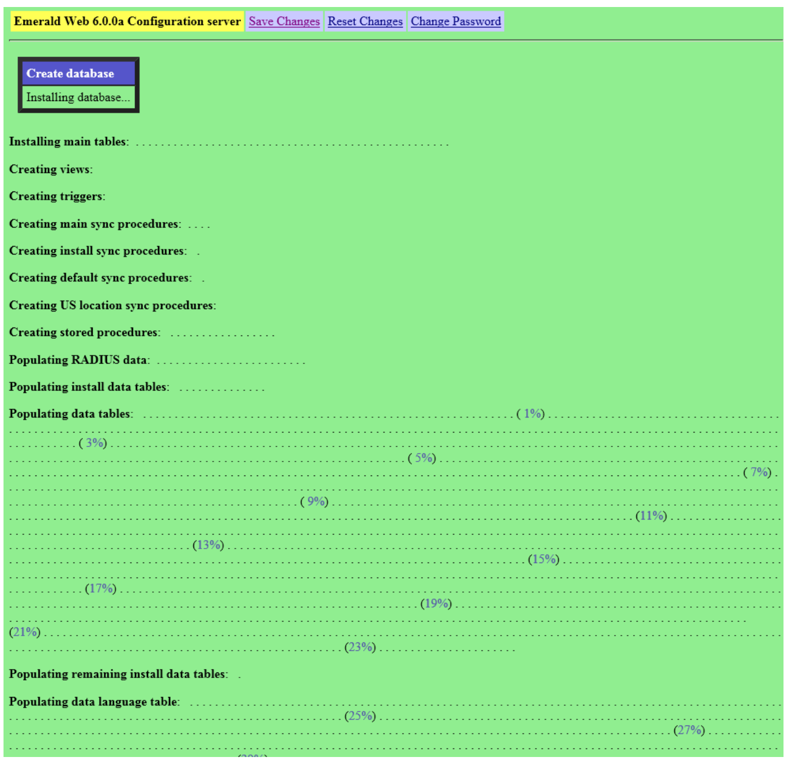
Field Descriptions are provided below. Some fields may not be available depending on the database server used.

Field	Description
Convert Emerald 5 database	If upgrading an existing Emerald 5 database then select a source Emerald 5 database to upgrade from. Emerald 5.0.73 or later is required to upgrade. Database conversion does not modify the existing Emerald 5 database in any way. Conversion is performed by creating a new Emerald 6 database copying data into converted Emerald 6 schema. During production cutover it is recommended all Emerald 5 related services be permanently shut down and Emerald 5 not be used at any time during or after the conversion process.
Copy Call History	Specifies the range of call records from the Emerald 5 database to import into the new Emerald 6 database.

Schema	To create a new database including upgrading from version 5 to version 6 schema must be set "Install". "Bypass" requires destination database to already contain an Emerald v6 schema having no MBRs. Procedure "DeleteALLAccounts" located in Emerald\sql\proc_extra.sql can be used to remove ALL account information from an existing Emerald 6 database. Bypass should not be used unless directed by an IEA support representative.

After the field values have been entered pressing Continue button initiates database creation and population of database with Emerald schema and default data.

As the database creation and conversion occurs, the following screen will be displayed showing the progress of the database creation. Once the process has completed successfully, the message "Emerald database installation complete" will be displayed at the bottom of the status screen.



Once database creation has been completed successfully:

1. If necessary from the ODBC control panel configure the data source to use the new database created.

2. From the 'database settings' menu main ODBC datasource and enter access credentials Emerald will use to access database server. Once completed clicking continue followed by save changes if successful allows Emerald application to be accessed by removing path information from existing browser URL.

THE EMERALD WEB CONFIGURATION SERVER

The Emerald Web Configuration Server was used during the installation process to install and configure the Emerald 6.0 database for the Emerald Management Suite. Although installation is the primary reason to use the Emerald Web Configuration Server, there are times where it may necessary to modify the Emerald configuration such as changing the database information, ODBC configuration and/or change the administrative operator passwords. The Emerald Web Configuration options are available any time by starting the Web Configuration Server by doing the following:

1. Start the Emerald Web Configuration Server.

   On Windows systems:

   a. If the Emerald Web Server is not started, select Web Server Debug Mode from the Start Menu/Program Files/Emerald/Server menu.

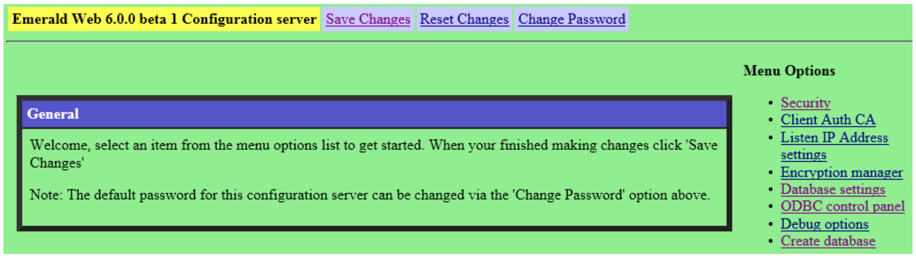
   b. To login to the Web Configuration Server, select Web Config from the Start Menu/All Programs/Emerald menu.

   On Linux systems:

   a. If the Web Configuration Server is not started, change to the /usr/local/emerald directory: "cd /usr/local/emerald" and execute the command "./emerwebsrv -config".

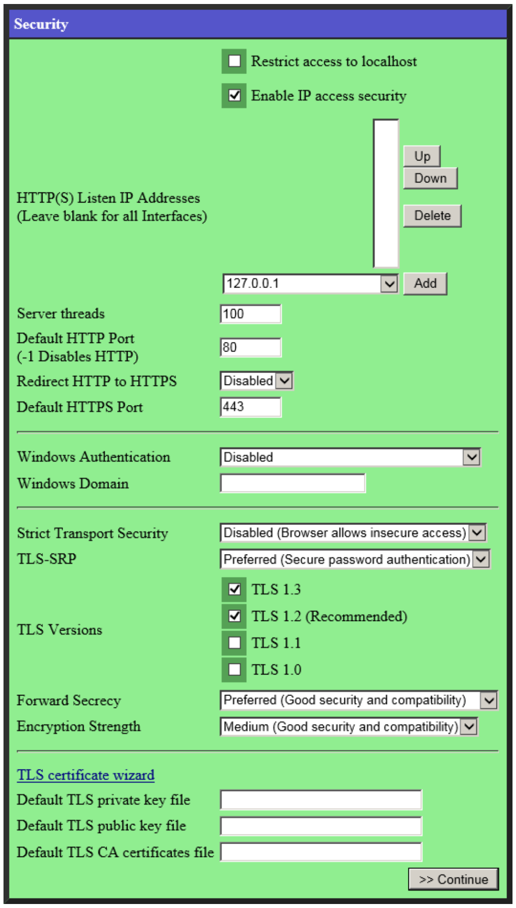
   b. Open a web browser and go to the URL: http://127.0.0.1/settings.

2. When prompted, enter a Username and provide the general Configuration Password provided during installation and initial start of the Web Configuration. Creation and access of this password is described above in the Initial Database Configuration section above.



Security

Security menu offers Emerald web server related listener and TLS configuration.



Field	Description
Restrict access to localhost	When checked Emerald web interface can only be accessed locally from a browser on the Emerald server by entering the local loopback (::1 or 127.0.0.1) address.
Enable IP access security	When enabled IP access security configured within Emerald Admin / Security / IP Security menu is enforced. When disabled all IP access security settings are ignored allowing operators to login from any source network.
HTTP listen IP address	A list of IPv4 and IPv6 interfaces Emerald web server is to listen for incoming web requests. The default and recommended setting is to leave list completely empty enabling Emerald to listen for incoming web requests on all available interfaces. If one or more listen interfaces are configured then Emerald configuration server will only be available from very first Interface on the interface list. Configuration server portion of the web interface will not be accessible when requested from any subsequent interfaces in the list. For example by setting the first listen interface to 127.0.0.1 configuration server may only be accessed from a browser on the Emerald server. When multiple listen interfaces are selected each interface is allocated a separate thread pool of "server threads" from which to process requests on that interface. This can be used to isolate external customer from internal operator facing users from competing for resources. For example while heavy demand or denial of service on external customer facing interface may impact access to the customer account center it would not impact availability for operators accessing Emerald via the internal interface. Listen addresses can also be used to configure separate TLS certificates for multiple domains or venues. When multiple listener addresses have been configured then per

	address certificate settings are configured from 'Listen IP Address settings' menu option.
Server threads	This setting provides an upper limit on the number of incoming web requests that can be processed concurrently. Please note this setting does not reflect number of operators able to be logged on and using Emerald at once. While typically sufficient default of 10 threads can be raised to improve performance and reduce any delays on busy systems where many operators or customers are accessing Emerald at once. It is recommended threads be set no higher than 100. Maximum configurable limit is 1024 threads.
Default HTTP Port	Port to be used for unsecured http requests to Emerald. By default http port is 80. Should Emerald be unable to listen on port 80 due to another web server listening on port 80 Emerald automatically falls back to listening on port 81 instead. It is recommended default http port be set -1 disabling HTTP access to Emerald once TLS certificates have been configured to minimize accidental attempts to access Emerald from an unsecured protocol.
Redirect HTTP to HTTPS	When enabled any unsecured requests to Emerald applications (*.ews files) are redirected to secured version. This redirect does not apply to requests for non-*.ews static content such as images and style sheets. Setting also does not apply when hosting Emerald as an ISAPI module on a third party web server platform. The following exceptions apply when redirect is enabled to minimize lockout risk: • If Emerald is accessed by IP address rather than DNS name redirect is not performed. • Should there be a problem preventing successful initialization of TLS such as a missing or invalid certificate pair then redirects are automatically disabled. Since this redirect mechanism is insecure its use is not recommended. Instead we recommend HSTS be enabled and all insecure HTTP access disabled by setting "Default HTTP Port" above to -1. HSTS provides a similar yet secure redirect function for requests to http to be upgraded to https. It is recommended operators take care to make sure all references to Emerald are in the form of secure URLs to minimize need for redirect.
Default HTTPS Port	Port to be used for secure http requests to Emerald. By default https port is 443. A TLS certificate must be installed before Emerald can be securely accessed using the https port.
Windows Authentication	When enabled any Emerald operator accounts with a blank password are authenticated using available Windows account databases such as local accounts or an active directory domain the Emerald server is a member. To move existing operators from Emerald to Windows authentication remove the password from operator account by entering keyword 'blank' into the password field of operator account form within Security / Operators menu. Operators with no passwords are listed with a gold background color. If an operator is currently logged on to Emerald when associated windows account is subsequently disabled operator continues to have access to Emerald until their currently active session is closed. At this point any further authentication would be denied. Active sessions can be closed from Web Interface / Active Sessions menu. Windows guest accounts either locally or on the domain must be disabled prior to using this feature. Emerald startup is suspended while both this feature is enabled and an active guest account is detected. This feature is not related to the ability to host Emerald under IIS and authenticate operators by leveraging integrated authentication features of IIS. When Emerald is hosted

	under IIS this feature would normally be disabled. Windows authentication is applicable to operators only and does not apply to customer account center. This feature is available only on the Windows platform.
Windows Domain	If windows authentication is enabled this controls domain that will be used for operator authentication. Emerald server must be a member of the domain. If there is no domain leave Windows domain field blank. This feature is available only on the Windows platform.
PAM Authentication	When enabled any Emerald operator accounts with a blank password are authenticated using available PAM account databases such as local accounts or a centralized directory server. To move existing operators from Emerald to PAM authentication remove the password from operator account by entering keyword 'blank' into the password field of operator account form within Security / Operators menu. Operators with no passwords are listed with a gold background color. If an operator is currently logged on to Emerald while associated PAM account is subsequently disabled operator continues to have access to Emerald until their currently active session is closed. At this point any further authentication would be denied. Active sessions can be closed from Web Interface / Active Sessions menu. PAM authentication is applicable to operators only and does not apply to customer account center. This feature is available only on the Linux platform.
PAM Service Name	Service name correspond with PAM configuration files located in the /etc/pam.d folder. To use PAM authentication a configuration file matching service name must be configured. For example if PAM Service Name is 'emerald' for operators to authenticate using the same databases as they would to login remotely via SSH the contents of file 'sshd' can be copied to file 'emerald' within folder /etc/pam.d. This feature is available only on the Linux platform.
Strict Transport Security (HSTS)	If enabled this feature provide a security "latch" preventing user browsers from allowing access to Emerald in an insecure manner after user has successfully logged on to Emerald securely while this setting was enabled. Normally enabling this setting has the following effects within the browser. • Any attempt to access Emerald via http is automatically rewritten and redirected as https • TLS certificate validation failure is unconditionally fatal. Users are NOT given the opportunity to manually "continue anyway" or set an exception if validation of any security aspect such as certificate chain, DNS name or certificate validity should fail. • This feature normally has the side effect of redirecting any request to any port matching DNS name to an https URL. This includes any other web servers that may be listening on different non-standard http ports such as RadiusNT/X Administrator (8011) or third party systems. The restriction only applies to URLs containing DNS name matching Emerald URL. • The setting cannot be undone or changed while any security aspect of TLS has failed. For example disabling this feature after a certificate has expired will not

<table>
<tr><td></td><td>restore access to clients willing to ignore security warnings who have previously logged on with this setting enabled. The setting can only be undone when disabled prior to a given user having successfully securely authenticated.</td></tr>
<tr><td>TLS-SRP</td><td>This feature enables secure password based authentication as well as subsequent network session encryption of operators with or without use of TLS certificates. This setting is intended for future secure API access and future browsers supporting secure password authentication. This feature may be disabled if not currently used.</td></tr>
<tr><td>TLS Version</td><td>Controls TLS version availability during TLS version negotiation between Emerald server and client browser.</td></tr>
<tr><td>Forward Secrecy</td><td>Forward secrecy offers protection of previously encrypted sessions from retroactive compromise by any future disclosure of the Emerald server's private key.

This setting does not apply to sessions using TLS version 1.3 where forward secrecy is mandatory. When using client certificates for two-factor authentication it is recommended forward secrecy set "Required".

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Disabled</td><td>Browsers are forbidden from negotiating cipher suites which offer forward secrecy.</td></tr>
<tr><td>Allowed</td><td>Browsers may select a cipher suite which offers forward secrecy however forward secrecy will not be used unless the browser both explicitly supports and prefers it over non forward secure ciphers.</td></tr>
<tr><td>Preferred</td><td>If browser supports forward secrecy then forward secure cipher will be used regardless of browser preference.</td></tr>
<tr><td>Required</td><td>If browser does not support forward secrecy then a secure session is not established and the connection fails.</td></tr>
</table></td></tr>
<tr><td>Encryption Strength</td><td>Imposes limits on acceptable cipher suites to be negotiated with browsers. Generally lower strength encryption provides better compatibility while still allowing more secure ciphers to be negotiated with browsers that support them. If a mutually acceptable cipher suite cannot be found then a secure session is not established and the connection fails.

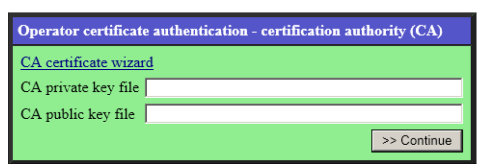
<table>
<tr><th>Strength</th><th>Description</th></tr>
<tr><td>Low</td><td>This setting provides the highest compatibility yet is very likely to fail any kind of security compliance scan. Low does not include intentionally weak algorithms such as "export" grade ciphers or anything known to be broken to the extent of risking practical bypass of secure cipher negotiation. This setting is intended to provide high compatibility with low "real world" technical risk.</td></tr>
<tr><td>Medium</td><td>Normal recommended setting offering good compatibility with slightly older and current browsers. Medium does not allow negotiation of ciphers with known weaknesses and is able to pass security compliance scans.</td></tr>
<tr><td>FIPS-140</td><td>Limits cipher selection based on US government FIPS 140 standard.</td></tr>
<tr><td>High</td><td>Offers negotiation of only highest available security at risk of limited browser compatibility.</td></tr>
</table></td></tr>
<tr><td>TLS certificate wizard</td><td>Launches a comprehensive certificate management wizard to assist with all key management tasks including creating private keys, certificate signing requests (CSRs), options for self-signed certificates and key validation.</td></tr>
<tr><td>Default TLS private key file</td><td>Fully qualified path + filename on the local filesystem containing the Emerald web servers RSA private key in Base64 format. It is recommended TLS certificate wizard be used to generate a private key.

This file contains private key data identified by a section starting with
-----BEGIN RSA PRIVATE KEY-----</td></tr>
</table>

	And ending -----END RSA PRIVATE KEY----- The BEGIN/END marks starting and ending with 5 dashes must not be removed from the private key file.
Default TLS public key file	Fully qualified path + filename on the local filesystem containing the Emerald web server's public key in Base64 format. This file is normally provided by your CA in response to a certificate signing request (CSR) generated by the TLS certificate wizard. This file contains public key data identified by a single section starting with -----BEGIN CERTIFICATE----- And ending -----END CERTIFICATE----- The BEGIN/END marks starting and ending with 5 dashes must not be removed from the public key file.
Default TLS CA certificate file	Fully qualified path + filename on the local filesystem containing the "intermediate" or "certificate chain" file in Base64 format provided by your CA. The CA file provides intermediate certificates linking root certs stored in the browsers trusted certificate database with the actual signer of your public key. This file is needed to establish the trust path from root to your public key. If not configured some browsers may be unable to accounting for the missing certificates preventing users from connecting to Emerald. This file contains a variable list of multiple BEGIN/END certificate sections formatted the same as Default TLS public key file above.

```
After making any changes within security menu it is necessary to click "Save Changes" and then restart Emerald web server service before changes can take effect.
```

Client Auth CA

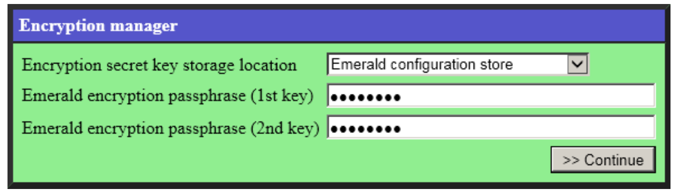


Client Auth CA is used to configure a certificate authority for purposes of issuing client certificates to Emerald operators supporting two factor authentications. CA certificates are generated by clicking 'CA certificate wizard' link following on screen instructions. Generating a CA certificate does not require you to obtain or purchase keys from a third party. When using client certificates it is recommended forward secrecy option within security menu be set "Required".

If Emerald is hosted on a third party web server or placed behind a reverse proxy only the generated CA public key should be imported into the third party system following vendor instructions for certificate authentication.

Encryption Manager

This menu configures database encryption key used to protect sensitive information including passwords, credit card and banking numbers. If database has been encrypted then valid encryption key(s) will be necessary to startup Emerald and related services requiring access to encrypted data.

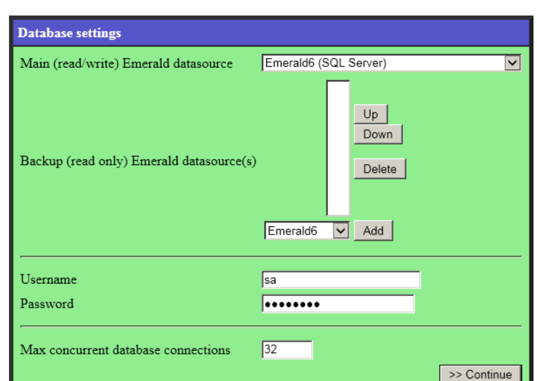


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Encryption key storage location</td><td>Depending on operating system and operating system version used following key storage options are available. If storage is changed data stored in the previous location is cleared.
<table>
<tr><th>Location</th><th>Description</th></tr>
<tr><td>Emerald configuration store</td><td>Entered key is stored in same configuration database as Emerald (Windows registry or ini file depending on operating system). Safety of stored key depends on successfully controlling access to configuration database.</td></tr>
<tr><td>Windows credential store</td><td>Entered key is stored in windows credential store. Safety of stored key depends on Windows syskey. Syskey modes requiring startup device or passwords can provide additional protections.

If windows credential store is used Emerald and all related services requiring access to encryption key must only run as user the key was set under. For example stopping an Emerald service and running it as a different user will fail because the encryption key is not available to any other user.</td></tr>
<tr><td>Disk filename containing secret key</td><td>Full path + filename of text file containing key is entered. Safety of stored key depends on successfully controlling access to file. File system security features such as disk encryption/EFS may be used to improve security of file.</td></tr>
</table></td></tr>
<tr><td>Encryption passphrase (1st key)</td><td>If there is only one encryption key enter it in the 1st key field and leave the 2nd key blank. 2nd key field is not a passphrase confirmation field. Do not enter the same key into the 2nd key field.</td></tr>
<tr><td>Encryption passphrase (2nd key)</td><td>If there are two encryption keys using "dual control" second operator should enter second key in this field. When two keys are used both are required. 1st and 2nd keys may be entered by any operator in any order. It is not necessary to remember which operator controls 1st vs 2nd key.</td></tr>
</table>

To confirm encryption keys have been accepted click save changes to validate configuration.

Database Settings

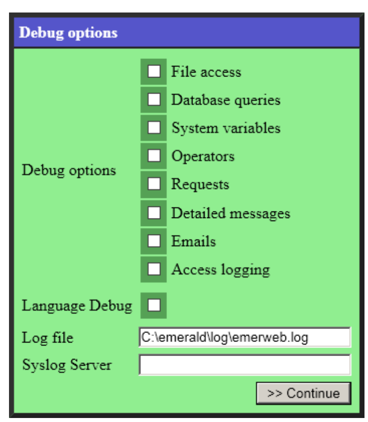


Emerald data is accessed via an ODBC datasource configured to establish connectivity to Emerald database. On Windows platforms it is recommended Windows 32-bit ODBC control panel from Start Menu / All Programs / Emerald / Operating System / ODBC Control Panel (32-bit) be used to configure database connectivity instead of the included ODBC UI.

Field	Description
Primary read/write datasources	ODBC system datasources that will be the primary read/write connection to the database. If the database is redundant with automatic read/write failover such as database mirroring or clustering redundancy can be configured within the ODBC datasource where supported or listed as separate datasources. Datasources are used in listed order based on availability.
Secondary read-only datasources	ODBC system datasources used for accessing backup read-only replicas of the database in event access to all main read/write datasources are unavailable. No changes can be made to any Emerald data when a backup datasource is used. If multiple backup datasources are available concurrent connections are balanced across all available datasources. It is recommended application intent be set 'read only' within ODBC configuration of datasources intended for read only use.
Secondary usage	"Failover" – secondary is only used when all primary datasources are unavailable. "Failover + offload read-only work from primary" – secondary datasources when available are also used to selectively offload certain read-only operations chiefly account searches, dashboards and most reporting to secondary databases in order to reduce utilization of primary databases. When using this feature care should be taken to ensure secondary databases remain sufficiently synchronized to avoid the presentation of stale or conflicting data within Emerald.
Username	Username if required to establish connection to Main and/or backup datasources
Password	Password if required to establish connection to Main and/or backup datasources
Max concurrent database connections	Maximum number of concurrent database connections per configured datasource that can be used by any single Emerald application at any point in time. This limit is a per application setting and is not a global limit on total number of concurrent database connections across all Emerald applications. Limit applies to Emerald Suite applications including Emerald web server, Emerald scheduler and billing engine. This setting does not affect RadiusNT/X.

Debug Options

Offers logging of informational events occurring within Emerald web server for troubleshooting and access logging. It is recommended normally debug options remain disabled unless needed. Important warning and error information is always logged regardless of enabled debug options.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Debug options</td><td>Enables logging of optional informational data to Emerald log file and syslog server.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>File access</td><td>Logs list of ews template files processed as a result of web requests. The list includes both file requested by operator and other template files included from top level ews template.</td></tr>
<tr><td>Database queries</td><td>Details about database queries executed while processing ews templates including query labels and execution time statistics.</td></tr>
<tr><td>System variables</td><td>Provides information about form variables and values of http GET and POST requests submitted to Emerald web server.</td></tr>
<tr><td>Operators</td><td>Information related to management and lookup of operator sessions based on incoming http requests to Emerald.</td></tr>
<tr><td>Requests</td><td>Incoming requested resource generally represents file name of ews template resulting from incoming http request. Logging is limited to requests related to ews templates. This does not include static content such as requests involving image or html files.</td></tr>
<tr><td>Detailed messages</td><td>Currently limited to providing a list of emerweb package files loaded into the memory package database during startup of Emerald web server.</td></tr>
<tr><td>Emails</td><td>Currently unused</td></tr>
<tr><td>Access logging</td><td>When enabled summary data is logged related to each incoming http request including requesting IP, timestamp, operator account, filename and per resource audit summary including general description of access and important variables associated with request. Access logging is very similar to access logs of web servers and can be useful for tracing activity of operators over time.</td></tr>
</table></td></tr>
<tr><td>Language Debug</td><td>When enabled annotates strings with String ID labels to assist operators in developing or customizing language translations. If this setting is changed it is necessary to restart Emerald web server for change to take effect.</td></tr>
<tr><td>Log file</td><td>Full path + filename where log entries are to be written on the filesystem local to Emerald web server. If log file is not specified default location Emerald/log/emerweb.log will be used. The following pattern substitutions may be used when configuring filename based on current date to provide for automatic rotation of log files.

<table>
<tr><th>Pattern</th><th>Description</th></tr>
<tr><td>YYYY</td><td>Current four digit year (2020)</td></tr>
<tr><td>YY</td><td>Current two digit year (20)</td></tr>
<tr><td>MM</td><td>Current month of year (07)</td></tr>
<tr><td>DD</td><td>Current day of month (10)</td></tr>
</table>
Example log file where a new log is created each month:
C:\program files\emerald\log\emerweb_YYYY_MM.log</td></tr>
</table>

	Emerald does not automatically remove or archive log files.
GBE Log file	Full path + filename where billing engine related log entries are to be written on the filesystem local to Emerald web server. If log file is not specified default location Emerald/log/gbe.log will be used. Pattern substitutions in table above for Log file are also applicable to GBE Log file.
Syslog Server	DNS name or IP address of syslog server to transmit log messages. If a DNS name is configured using a DNS name having multiple IP addresses of the same address family syslog messages are broadcasted to each IP address of the same family associated with DNS name. When enabled log messages are transmitted to syslog server in addition to Log file configured above. All syslog messages from Emerald are transmitted using facility LOCAL2 and a severity of NOTICE regardless of type or content of message. Transmitted syslog messages are not encrypted, acknowledged or authenticated. It is not recommended syslog be transmitted over the Internet.

LAUNCHING AND LOGGING ON TO EMERALD

To launch Emerald:

On Windows systems select "Web Login" from Start Menu/All Programs/ Emerald. Alternately start a web browser on Emerald server and browse to the URL: http://localhost

When logging on to Emerald for the first time use default username and password of '**admin**' and '**pass1**' respectively to access Emerald. Default password **should be changed as soon as possible** from Emerald Admin / Security / Operators menu.

COMMON FIELDS

Following fields commonly appear in configuration menus throughout Emerald admin.

Field	Description
String ID	Used to provide language translations for a configuration item. If translation is necessary a custom string id for translation of the items description may be added using Emerald Admin / Web Interface / Languages / English - Add Data. Once String ID has been added translations for each language can be configured. Note any translation related changes requires Emerald web server service to be restarted to take effect. Translations are visible throughout Emerald Client, Customer Center and Signup Server interfaces.
Billing Group	Typically when a Billing Group is set the configuration items availability is restricted only to MBRs assigned to the same group. For example two ISPs are managed from an instance of Emerald using billing groups "ISP A" and "ISP B". A new service type "Wireless (ISP B)" is created having service type billing group set "ISP B" restricting availability of "Wireless (ISP

	B)" service to only "ISP B" customers.
Service Group	If a service group is selected configuration item is available to any billing group associated with the selected service group. Service group membership applies in addition to matching the configuration items billing group field. For example if an item is assigned to billing group A and the selected service group of the same item is associated with groups B and C then configuration item is accessible to billing groups A, B and C.
Access Label	Restricts access to configuration items based on rights of operator group an operator is assigned. For example the service 'Employee Wireless' may require a supervisor to provision and will not be available for selection to technical and billing staff. Access labels are configured from Emerald Admin / Security / Access Labels
Sort Order	Adjusts sequence configuration items are displayed both in administrative menu and the Emerald client when selecting configuration options. Items are sorted in ascending order with values starting 0 thru 32767. Items sharing the same sort orders are sorted alphabetically by the items description field. It is recommended when assigning sort orders to include gaps in ordering to account for any future expansion. Most configuration items can be hidden from view and made unavailable for further selection by setting items sort order to a negative value. When sort order is negative the item appears with the inactive background color.
Access Time or Time Range	While role of this field is unique to each configuration item the field is used to specify range of calendar days and time of day using natural language form with the following limitations. • Year should not be specified. All ranges apply to any year • MMDD - MMDD pattern may be used only once per time range (Jan 1 - Feb 1) • English is currently only supported language • Month names must be spelled out (Jan or January…) • Time of day must use format HH:MM (3:00 or 3:00 AM) Examples of valid time ranges can be found below.

Example	Comments
Dec 24,25	Months may be abbreviated.
Feburary 28	Common misspellings are supported.
Last Monday of May	First, 1st, second, 2nd, third, 3rd, fourth, 4th and last can be used to describe week of month.
Dec 10 thru Feb 15	Date and time automatically wraps around day, week, month and year boundaries.
May, June, July 1 thru 20	Covers the 1st thru 20th of the months of May, June and July.
Sep-May Mon-Fri 8:00 AM - 5:00 PM	Range of time of day, month and days of week can be specified concurrently.
Jan - Feb, March, April, May - Oct, Nov, Dec Mon thru Wednesday, Thursday and Fr	Multiple ranges are allowed for month, month day and day of week. Only one range is supported for time of day or MMDD - MMDD pattern is used like the "Dec 10 thru Feb 15" example above.
1:00 thru 22:00	Without specifying 'AM' or 'PM' military time is assumed.
10:00 PM to 7:00 AM	Wrap around time of day.
5	5th day of any month.
1 2 3 4 5-8, 9, 10	1st thru 10th day of any month.

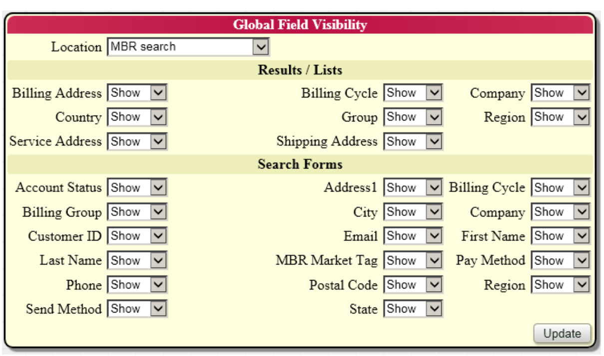
<table>
<tr><td></td><td>
<table>
<tr><td>M-F 9:00 AM - 5:00 PM</td><td>Covers 9:00 AM thru 5:00 PM for weekdays Monday thru Friday.</td></tr>
</table>

Examples of invalid incorrectly formatted time ranges.

<table>
<tr><th>Invalid Time Range</th><th>Reason</th></tr>
<tr><td>9AM - 10PM</td><td>Time of day not in HH:MM format and space required before AM/PM.</td></tr>
<tr><td>1/1 thru 3/20</td><td>Month name is required.</td></tr>
<tr><td>Jan 1 - Jan 10, Feb 5 - Feb 15</td><td>Only one MMDD - MMDD range pattern is allowed.</td></tr>
<tr><td>1:00 AM - 7:00 AM, 8:00 PM - 11:00 PM.</td><td>Only one time of day range pattern is allowed.</td></tr>
<tr><td>Jan 1 2017 - Jan 1 2018</td><td>Year not allowed.</td></tr>
</table>
</td></tr>
<tr><td>External Ref</td><td>Commonly used as a key to link a configuration item within Emerald to an external database or process.</td></tr>
<tr><td>IP Address Range</td><td>Address ranges are supported in any of the following forms:

<table>
<tr><th>IP Version</th><th>Format</th><th>Example</th></tr>
<tr><td>IPv4</td><td>Single address</td><td>192.168.0.1</td></tr>
<tr><td>IPv4</td><td>CIDR range</td><td>10.0.0.0/8</td></tr>
<tr><td>IPv4</td><td>Wildcard octet</td><td>10.20.*.*</td></tr>
<tr><td>IPv4</td><td>Address range</td><td>10.0.100.10 - 10.0.100.20</td></tr>
<tr><td>IPv6</td><td>Single address</td><td>2001:db8::1</td></tr>
<tr><td>IPv6</td><td>CIDR range</td><td>2001:db8::/64</td></tr>
<tr><td>IPv6</td><td>Address range</td><td>2001:db8::1 - 2001:db8::f</td></tr>
</table>
</td></tr>
</table>

Field Visibility



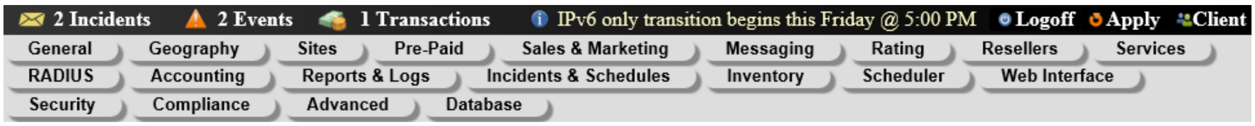
Field visibility enables fields throughout Emerald client interface to be selectively displayed or hidden based on configuration and operator preferences to better meet needs of organization and individual operators. Visibility is configurable on a number of levels including Global, Billing Group, Service Type, Operator Group, Operator, Address Type and others. No priority is given to any configuration level. Please note details of each visibility option below to fully understand possible outcomes should competing field visibility settings exist.

Visibility Setting	Description
Default	Indicates no preference for or against visibility of field. Normally for all configuration levels except global default will be heavily used with "Show" or "Hide" selected only to override global defaults. For a field to be visible at least one configuration level must be "Show" rather than default. If all levels are "Default" or if any level is "Hide" the field will not be visible.
Show	Indicates a preference for the field to be visible. If set the field will be visible unless any

	other level is "Hide" in which case the field shall not be visible.
Hide	Indicates a demand for field to not be visible. If set the field will not be visible regardless of field visibility settings of any other configuration level.

EMERALD ADMINISTRATIVE MENU OPTIONS

The Emerald Administrative options are used to configure the billing and account selections available throughout the Emerald Management Suite. After making changes within Emerald Administrative menu select "Apply" to refresh running configuration of Emerald UI and related services.



The following map offers a quick overview of main administrative menu options:

Menu Item	Purpose
General	Configuration of billing groups, service groups and organizations used to organize groups of accounts. General menu also includes configuration of Internet domains, administrative addresses, file attachments and MBR level custom data.
Geography	Manages regions, types of customer addresses, geocoding and geography
Sites	Defines administrative addresses, sites and towers
Pre-Paid	Provides for the batch creation and management of prepaid vouchers
Sales & Marketing	Informational settings for sales persons, commissions and referrals. Service affecting configuration includes discounts, promotional codes and market tags.
Messaging	Configuration of Email and SMS interfaces, bulk messaging profiles and account notifications.
Rating	Provides for the management of usage-based rating of call records, network flows as well as third party data. The Rating menu includes the definition of Rates, Rule Sets, Time Sets, Rate Classes, Intervals and Data Sources
Resellers	Used to define multi-organization grouping and reseller configured service pricing. The Resellers menu includes the definition of organizations, billing groups and reseller service pricing.
Services	Service categories and service types, service level custom data and external system integration
RADIUS	Manages RadiusNT/X related configuration including attributes, access servers, roaming, attribute filtering and session management
Accounting	Most of Emerald billing and payment processing related configuration is managed from this menu. Options include billing settings, charge types, pay periods, taxes, billing cycles, send methods, GL codes, CC/EFT batch processing, late fees, time & data charges, payment types and plans.
Reports & Logs	Offers configuration of reports, log data retention, change logging, syslog filtering and classification, external alerting and gauge data management.
Incidents & Schedules	Includes configuration of incidents and incident assignment, scheduling resources and events.
Inventory	Setup of warehouses for inventory storage, products, product categories and subcategories and related product attributes and states.
Scheduler	Provides configuration, status and historical search of scheduled tasks required for automation and maintenance of the Emerald system.
Web Interface	Configuration of web interface related settings including: View and remove active operator

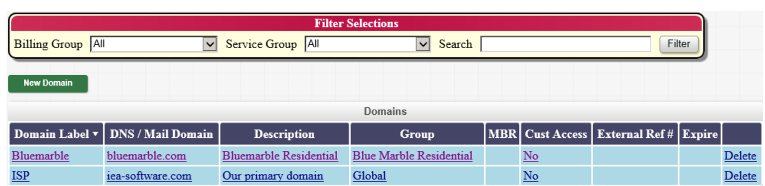
	sessions, theme and signup server setup, hyperlinks, client settings and search limits, license keys, language translations, reverse proxy configuration and upgrade & test safing.
Security	Offers setup of operator accounts and related permissions and privileges, IP based access restrictions, database field encryption and trusted access.
Compliance	Configuration checking and reporting related to industry standards and government regulatory compliance.
Advanced	Menu items in this area are not documented, supported or intended to be managed or changed by operators. It is recommended settings within this area only be altered when directed by IEA support staff.
Database	This area is used to run database queries and export associated data, review current database activity, obtain statistics related to index and data storage, view current database server log and schedule regular database backups when using SQL Express.

GENERAL CONFIGURATION

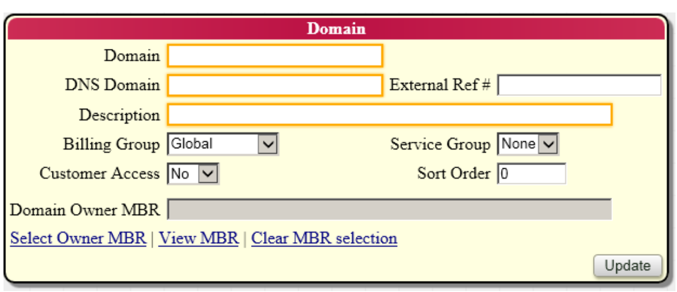
General menu offers configuration of billing groups, service groups and organizations used to organize related accounts. General menu also includes configuration of Internet domains, administrative addresses, file attachments and MBR level custom data.

Domains

Domains represent Internet domain names. Any names your organizations are affiliated with are normally defined. Domains can also include Internet names owned by specific customers. Domains are selected when creating new services within an MBR.



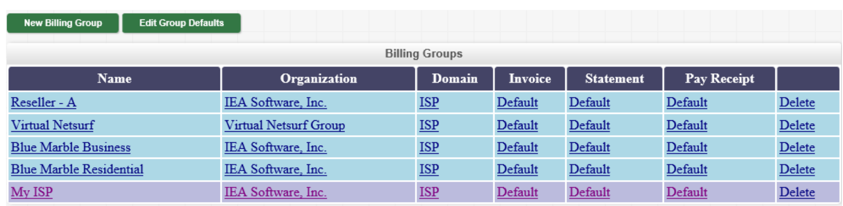
If a domain has been assigned to an MBR the domain is only available for selection to services of that MBR. Domain determines default realm for RADIUS authentication when a realm name is used during authentication. Domains can also be used for managing domain registration and hosted service provisioning.



Field	Description

Domain	Choose a name for Emerald to reference the domain.
DNS Domain	Enter the full Internet domain address, such as "iea-software.com".
External Ref	See Common fields
Description	Enter a short domain description, or note of comment.
Billing Group	See Common fields
Service Group	See Common fields
Customer Access	When ‘Yes’ this Domain is available for selection by the end user when adding a new account via the manage accounts menu within the customer account center. Note: In order for users to be able to choose domains the service type must have the ‘Allow Customer Set Domain’ package permission enabled.
Sort Order	See Common fields
Domain Owner MBR	Setting a domain owner enables only the specified MBR to use this domain when adding new services to the MBR. When a Domain owner is chosen the Domain cannot be used by any other MBR or as a default setting for Billing Groups, Signup Servers and Prepaid cards. If a Domain is already used as a default it is unavailable to be assigned to a specific MBR and the Domain Owner dialogue is not shown.

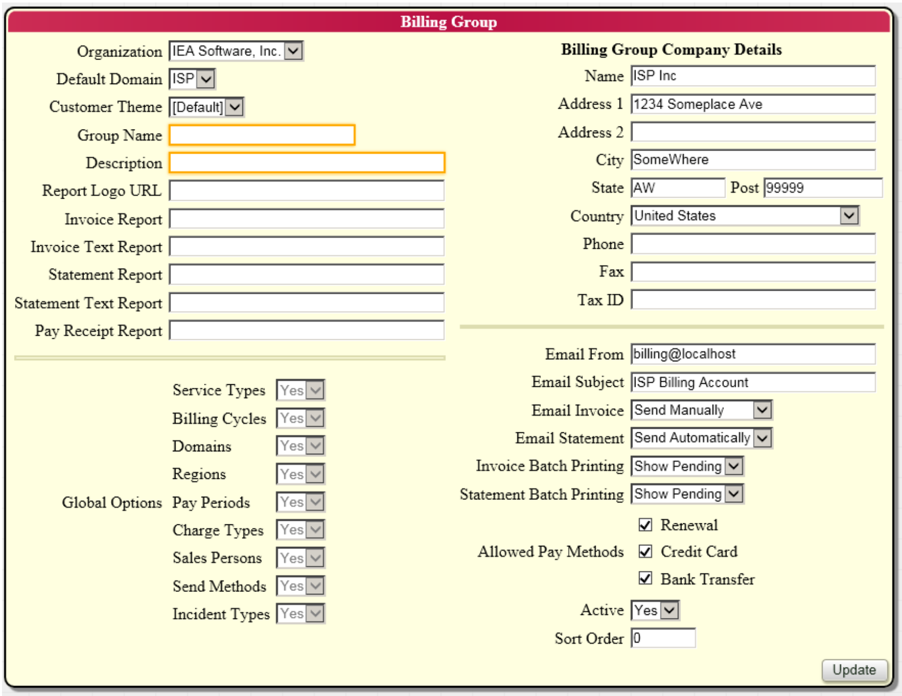
Billing Groups



A Billing Group defines a set of MBRs having common billing characteristics. Billing Groups are important to Emerald’s configuration because they allow different billing features, reporting, access controls and options to be designated to only a subset of MBRs sharing a common billing group.

Billing groups are commonly used to partition customer types for example "Residential Customers" vs "Business Customers" or to support partitioning of multiple organizations, resellers or venues within a common instance of Emerald. (e.g. "ISP A", "ISP B", "Reseller C")

The particular billing group assigned to an MBR is able to affect availability of most configuration choices when managing MBRs and services. When combined with themes, group level operator access controls, customized invoices and payment processors it is possible to offer a wide range of scenarios from simply organizing related accounts to isolating organizations with separate customers and staff within common instance of Emerald.

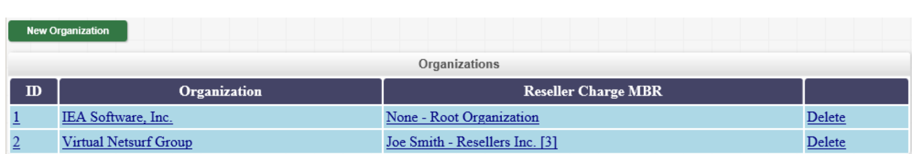


Field	Description
Organization	Organization the billing group is to be associated with.
Default Domain	Choose a default domain for this Billing Group. When the Billing Group is later assigned to an MBR, the domain specified here will be supplied as the default domain value on the MBR Service account screen (the default may be over-ridden) and can subsequently also be used to determine user default email addresses.
Customer Theme	If a theme is selected the chosen theme is preferenced when an end user within this group logs into the customer account center. The setting does not apply to the signup server or operator interface.
Group Name	Name of the billing group to appear in selections referencing this group throughout Emerald.
Description	Short informational text offering more detail about this group
Report Logo URL	For HTML rendered reports this sets a remote image URL for display on customer invoices, statements and some custom reports.
Invoice Report	Select the report format to use for the generation of mailed/printed invoices for MBRs of this billing group. This option allows customization of invoice format per billing group. If no Invoice Report is provided, the general Billing Group Default Invoice Report will be used for this Billing Group.
Invoice Text Report	Select the report format to use for the generation of emailed invoices for MBRs of this billing group. If no Invoice Text Report is provided, the general Billing Group Default Invoice Text Report will be used for this Billing Group.
Statement Report	Select the report format to use for the generation of mailed/printed statements for MBRs of this billing group. This option allows customization of statement format per billing group. If no Statement Report is provided, the general Billing Group Default Statement Report will be used for this Billing Group.
Statement Text Report	Select the report format to use for the generation of emailed statements for MBRs of this billing group. If no Statement Text Report is provided, the general Billing Group Default Statement Text Report will be used for this Billing Group.
Pay Receipt Report	Report to be used for rendering payment receipts for payments to MBRs within this billing group. If not configured default payment receipt report is used.
Global Options	Choose "Yes" to allow MBR field selections for this billing group to include Global options, as well as the options specific to the billing group. Choose 'No' to restrict the MBR field selections to only

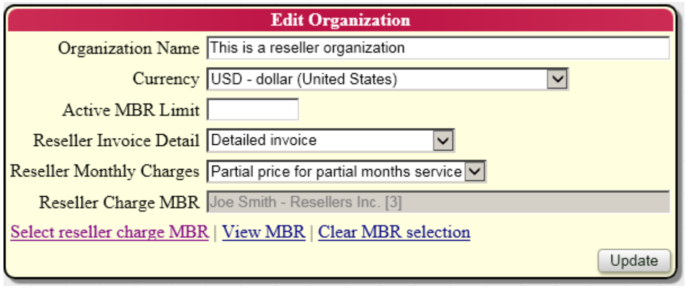
	those specifically set up for this billing group.
Allowed Pay Methods	Controls those pay methods available to MBRs within this billing group.
Sort Order	See [Common fields](#)
Active	Intended to temporarily disable network access for all services within the billing group.
Billing Group Company Details	Provide the Company name and address information to use for this Billing Group's billing document generation and distribution. This option provides the ability to track company name and address information associated with external entities that you have established as Emerald Billing Groups.
Email From	Enter the email address from which billing items are to be sent from (identifies the sender to the email recipient) for members of this Billing Group.
Email Subject	Enter the subject that should be included on all emailed billing correspondence for members of this Billing Group.
Email Invoice	This setting specifies how Invoices are sent via email for all MBRs within the billing group having an email send method. When set "Send Automatically" Invoices will be emailed when emailing "All" billing groups from the "Client" / "Billing" / "Send Bills" menu or automatically when scheduled via the Emerald task scheduler. When set "Send Manually" the specific billing group must be selected from the "Client" / "Billing" / "Send Bills" menu. When set "Sending Disabled" it is not possible to email invoices automatically for a billing group however individual invoices can be emailed manually from the MBRs invoices menu. This billing group level option can be overridden by send method configuration.
Email Statement	This setting specifies how Statements are sent via email for all MBRs within the billing group having an email send method. When set "Send Automatically" Statements will be emailed when emailing "All" billing groups from the "Client" / "Billing" / "Send Bills" menu or automatically when scheduled via the Emerald task scheduler. When set "Send Manually" the specific billing group must be selected from the "Client" / "Billing" / "Send Bills" menu. When set "Sending Disabled" it is not possible to email statements automatically for a billing group however individual statements can be emailed manually from the MBRs statements menu. This billing group level option can be overridden by send method configuration.
Invoice Batch Printing	When set "Hide Pending" any invoices that are pending for printing for postal delivery from the Emerald billing / send bills menu will not be displayed for this billing group. Setting "Hide Pending" is useful for situations where only statements are mailed out to the end user and invoices only need to be printed manually from each MBRs invoicing menu. When set "Show Pending" any invoices pending for printing for postal delivery for the billing group is displayed in the Emerald billing / send bills menu. This billing group level option can be overridden by send method configuration.
Statement Batch Printing	When set "Hide Pending" any statements pending for printing via postal delivery from the Emerald billing / send bills menu will not be displayed for this billing group. Setting "Hide Pending" is useful for situations where only invoices are mailed out to end users and statements only need to be printed manually from each MBRs statements menu. When set "Show Pending" any statements pending for postal delivery for the billing group is displayed in the Emerald billing / send bills menu. This billing group level option can be overridden by send method configuration.

Organizations

Much of Emeralds support for multiple service providers and reseller billing are based on



"Organizations". Organizations are a grouping of "Billing Groups" owned by the same entity. Organizations separate the monies managed by each company for reporting purposes, define the currency used throughout each organization and provide for the configuration of reseller relationships where an Organization is able to be billed for the services they provide by a parent organization.



Field	Description
Organization Name	Reflects the name of the company or branch.
Currency	Determines the currency type of all accounts associated to this organization. This currency information is used for reporting and by some credit card processors.
Active MBR Limit	This option places a limit on the number of Active MBRs that can be associated to the organization. MBR limits are useful for managing the allocation of Emerald MBR licenses.
Reseller Invoice Detail	When billing an Organization for their service usage this option controls the level of detail of the invoice presented to the "Reseller Charge MBR". "Detailed invoice" provides a line item for each service billed. "Summary invoice by service type" provides a smaller summary invoice with a quantity multiplier for each service type used.
Reseller Monthly Charges	When billing an Organization for their service usage this option controls how services created or closed part way through the month are handled. "Partial price for partial month's service" bills at a rate proportional to the fraction of the month the service were active. "Full price for partial month's service" bills the entire monthly rate to the reseller for services that were active for any length of time throughout the month.
Reseller Charge MBR	When billing an Organization for their service usage this option sets the MBR in the parent organization that is to be charged for the service usage of this organization. This MBR generally reflects the reseller.

Configuring General Billing Group Default Values

If you will be managing many different billing groups with similar configuration click "Edit Group Defaults" available from Billing Groups menu to set default group configuration. These default settings are applied whenever new billing groups are created.

Restricting Accounting options to a specific Billing Group

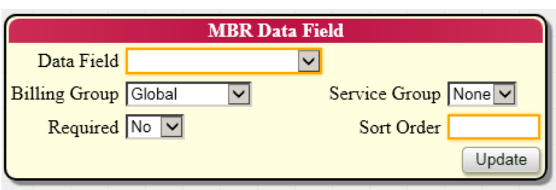
Emerald allows restricting certain Accounting and Global billing options to a specific Billing Group. Once associated to a specific Billing Group that option will only be available to MBRs of that Billing Group or those under a Billing Group with Global options.

Once one of the following types of Accounting or Global option entries has been created, it can be individually associated to a particular Billing Group: Service Type, Region, Billing Cycle, Pay Period, and Discount. A Billing Group can have any number of billing options associated with it. The Billing Group assignment is performed on the particular option entry screen by selecting a Billing Group from the presented Billing Group pick list, an example using the Region option is shown to the right. If the default 'All Groups' option is selected on the option screen, the option entry will remain available to all MBRs, regardless of Billing Group.

On new and existing Billing Group entries, you may find a message displayed within the group entry indicating, for example: 'No Service Type assigned to this group'. This is a status message indicating that no specific options of this type (for example: Service Type, Billing Cycle, Region) have been restricted to this Billing Group. This is just an informational message and requires no action, as it is not mandatory to restrict any options to a specific Billing Group.

MBR Custom Data Fields

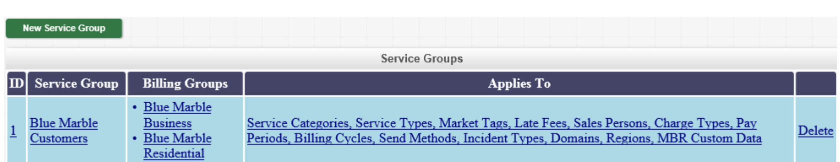
Custom data fields allow you to define extra fields of information your organization would like to track for each MBR. Extra MBR data fields chosen here shall be presented within the "Show MBR" detail display and MBR edit form allowing Emerald operator to optionally enter a value for each of the additional MBR data fields. MBR Custom data fields typically have only an informational role only used by Emerald for reporting and tracking purposes.



Field	Description
Data Field	This entry will be displayed as the label for the Custom Data field on the MBR account entry screen. Available data fields are configured from the "Manage Data Fields" option within MBR Custom Data menu.
Billing Group	See Common fields
Service Group	See Common fields
Required	Requires an operator to enter a value for this custom data field before they are able to save changes to the MBR.
Sort Order	See Common fields

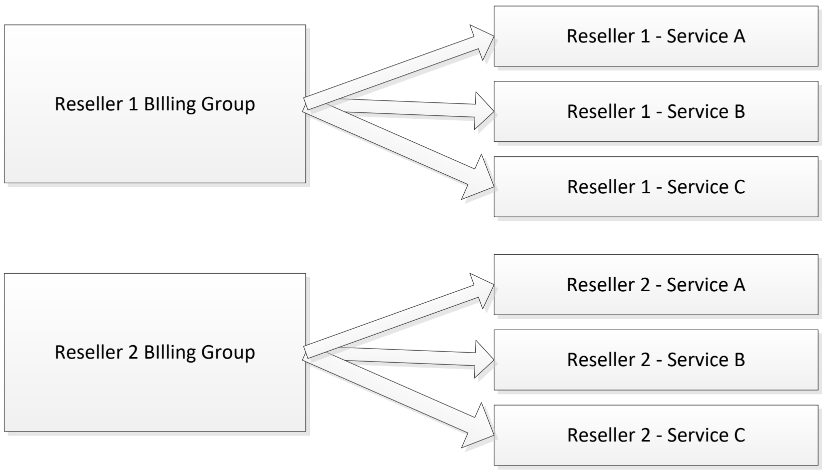
Service Groups

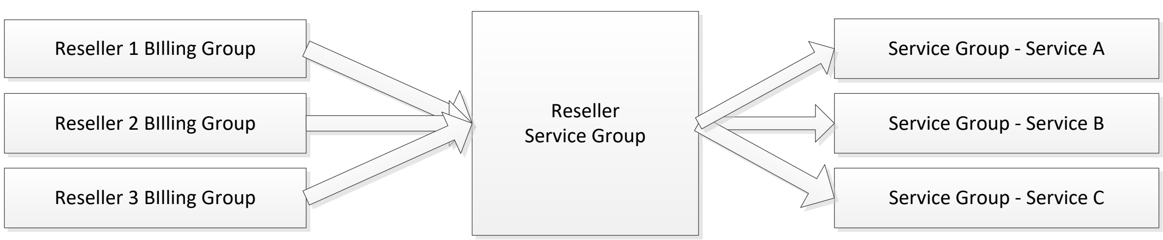
To better support systems with large numbers of billing groups service groups enables related billing groups to be bundled together for the purposes of configuring certain



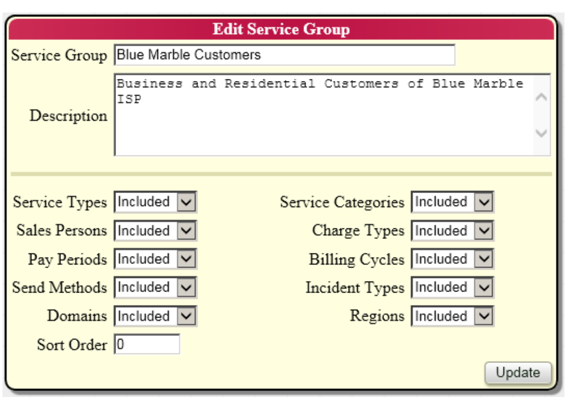
configuration options such as service types, pay periods and charge types without having to create duplicate configuration options for each billing group.

For example let's assume Reseller 1 and Reseller 2 is each assigned a similar set of service types. Service Types A, B and C. To support each reseller this scenario requires a total of 6 service types (2 resellers * 3 service types) created.





With service groups all similar resellers billing groups are assigned to a service group reducing the number of service types needing to be configured from 6 for 2 billing groups or 9 for 3 billing groups to 3 regardless of the number of billing groups assigned.



Service Groups apply only in an additive fashion to the traditional assignment method where items such as service types are either assigned specifically to a billing group or available globally to all billing groups having global options enabled. Please see "Admin" / "General" / "Billing Groups" for additional information.

The use of service groups is optional and not recommended if the Emerald system contains a small number of billing groups or billing groups used generally for the purpose of restricting operator access.

Field	Description
Service Group	Text uniquely describing the service group. This text will appear in selection lists throughout the Emerald administrator when configuring one of the "Included" items below.
Description	Text describing the purpose and use of this service group
Service Categories	When "Included" this service group is available for selection when configuring service categories. See "Admin" / "Services" / "Service Categories"
Service Types	When "Included" this service group is available for selection when configuring service types. See "Admin" / "Services" / "Service Types"
Market Tags	When "Included" this service group is available for selection when configuring market tags. See "Admin" / "Sales & Marketing" / "Market Tags"
Late Fees	When "Included" this service group is available for selection when configuring late fees. See "Admin" / "Accounting" / "Late Fees"
Sales Persons	When "Included" this service group is available for selection when configuring sales persons. See "Admin" / "Sales & Marketing" / "Sales Persons"
Charge Types	When "Included" this service group is available for selection when configuring charge types. See "Admin" / "Accounting" / "Charge Types"
Pay Periods	When "Included" this service group is available for selection when configuring pay periods. See "Admin" / "Accounting" / "Pay Periods"
Billing Cycles	When "Included" this service group is available for selection when configuring billing cycles. See "Admin" / "Accounting" / "Billing Cycles"
Send Methods	When "Included" this service group is available for selection when configuring send methods. See "Admin" / "Accounting" / "Send Methods"
Incident Types	When "Included" this service group is available for selection when configuring incident types. See "Admin" / "Incidents & Schedules" / "Incident Types"
Domains	When "Included" this service group is available for selection when configuring domains. See "Admin" / "General" / "Domains"
Regions	When "Included" this service group is available for selection when configuring regions. See "Admin" / "Geography" / "Regions"
MBR Custom Data	When "Included" this service group is available for selection when configuring MBR custom data fields. See "Admin" / "General" / "MBR Custom Data"
Sort Order	See Common fields

Batch Manager

History of prior batches of invoices, statements, payment imports and printing can be reviewed from batch manager. Historical data includes batch status, total number of items in batch, overall costs, operator and any related messages.

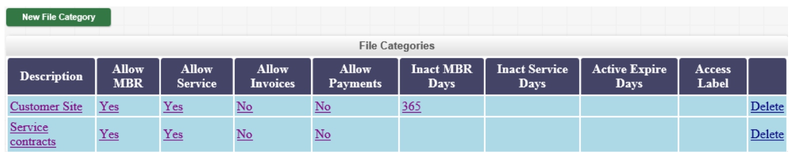
ID	Type	Status	Group	Operator	Date	Info	Item Count	Total Amount	
1	Invoice	Succeeded		admin	08/03/16 23:41:18		0	0.00	
2	Print Statement	Open	My ISP	admin	10/20/16 09:44:41		2	118.50	Delete
3	Invoice	Succeeded		admin	10/28/16 22:43:33		2	126.00	
4	Invoice	Succeeded		admin	10/28/16 22:43:36		1	37.05	
5	Invoice	Succeeded		admin	10/28/16 22:43:37		1	37.05	
6	Invoice	Succeeded		admin	10/28/16 22:43:38		0	0.00	
7	Invoice	Succeeded		admin	10/28/16 22:43:39		0	0.00	
8	Statement	Succeeded		admin	10/28/16 22:44:38		3	0.00	
9	Statement	Succeeded		admin	10/28/16 22:44:39		0	0.00	

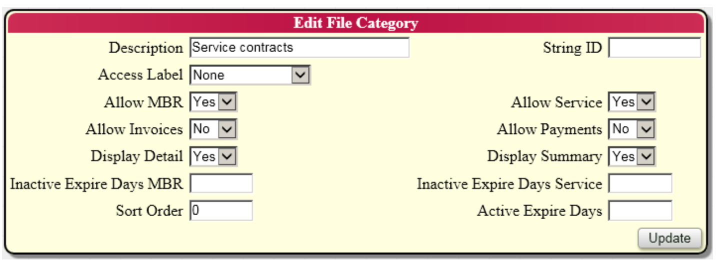
Batch manager also provides for operators to void a batch of invoices or reopen prior print queue items should there ever be a need to reprint a set of previously printed invoices or statements for postal delivery.

Field	Description
Batch ID	Filter search results by unique ID assigned to each batch run
Starting	Filter search results by batches created on or after the specified date
Ending	Filter search results by batches created prior to the specified date
Operator	Filter search results by operator responsible for batch creation
Batch Type	Filter search results by batch type (e.g. Invoices, Statements, Payments, Printing)
Current State	Filter search results by current status of a batch

File Categories

When files are uploaded for storage within an MBR file categories provide for organization of file attachments by role. With each category limits on acceptable file types, file expiration and MBR/Service level requirements can be defined.

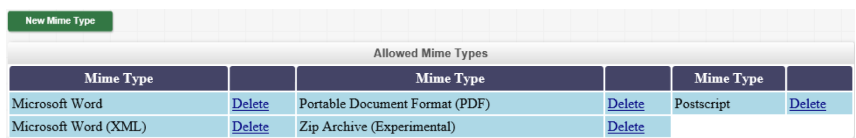




Field	Description
Description	Unique label describing type and purpose of file attachments. When uploading a file attachment within an MBR or service this field is displayed for category selection.
String ID	See [Common fields]
Access Label	See [Common fields]
Allow MBR	When "Yes" file category may be used for files attached to the MBR itself.
Allow Service	When "Yes" file category may be used for files attached to individual services within an MBR.
Allow Invoices	When "Yes" file category may be used for files attached to individual invoices within an MBR.
Allow Payments	When "Yes" file category may be used for files attached to individual payments within an MBR.
Allow Sites	When "Yes" file category may be used for files attached to sites within Sites / Sites menu of Emerald Admin.
Allow Towers	When "Yes" file category may be used for files attached to towers within Sites / Towers menu of Emerald Admin.
Allow Events	When "Yes" file category may be used for files attached to events within support menu of Emerald client.
Display Detail	Indicates file contents may be displayed automatically while showing detailed information specific to file or item file is attached. This field is currently unused.
Display Summary	Indicates file contents may be displayed automatically in list views of files or attached items. This field is currently unused.
Inactive Expire Days MBR	If set file attachments of this category assigned to MBR, Invoice or Payment levels are automatically deleted once MBR has been inactivated for more than configured number of

	days. To disable automatic removal of files based on MBR active status this field should be left blank.
Inactive Expire Days Service	If set file attachments of this category assigned to Services are automatically deleted once MBR or Service have been inactivated for more than configured number of days. To disable automatic removal of files based on Service active status this field should be left blank.
Sort Order	See Common fields
Active Expire Days	If set the attachment is automatically deleted once set number of days has passed from time of initial file upload. Active expire days applies unconditionally regardless of account status or any other factor. To disable automatic removal of files based on time of initial upload this field should be left blank.

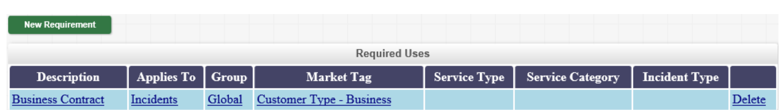
Allowed Mime Types



Once a file category is added accepted formatting of uploaded files can be restricted by adding one or more allowed mime types. If no allowed mime types are configured then no format restrictions are enforced on uploaded files. Additional mime types not in the list can be configured from "Emerald Admin" / "Advanced" / "Mime Types".

File type is determined by the uploading browser and or client operating system. Type determination for the same files may vary between browsers and operating systems. Mime type transmitted at time of upload is used when file attachments are subsequently downloaded. Emerald does not perform any checking of file content to determine whether mime type matches file content.

Required Uses



Once file category is established MBR and service level file requirements can be configured alerting operators to file attachments required to support specific types of MBRs and services.

Field	Description
Description	Label describing purpose of requirement. This field is informational only.
Applies To	Specifies whether requirement applies to MBR or service level.

<table>
<tr><td></td><td>
<table>
<tr><th>Applies To</th><th>Description</th></tr>
<tr><td>MBR</td><td>Requirement applies at the MBR level. Requirements are displayed as MBR alert and within MBR attachment menu.</td></tr>
<tr><td>Service</td><td>Requirement applies at service level. Requirements are displayed as a service alert and within the services attachment menu.</td></tr>
<tr><td>Incidents</td><td>This option is reserved for future use</td></tr>
</table>
</td></tr>
<tr><td>Billing Group</td><td>Restricts requirement to a specific billing group</td></tr>
<tr><td>Market Tag</td><td>When "Applies To" is MBR file requirement is restricted to MBRs where selected MBR level market tag is currently active.

When "Applies To" is Service then file requirement is restricted to Services where selected Service level tag is currently active.</td></tr>
<tr><td>Service Type</td><td>Restricts requirements to a specific service type.</td></tr>
<tr><td>Service Category</td><td>Restricts requirements to services of a specific service category.</td></tr>
<tr><td>Incident Type</td><td>Restricts files requirement to specific incident type. This option is reserved for future use.</td></tr>
</table>

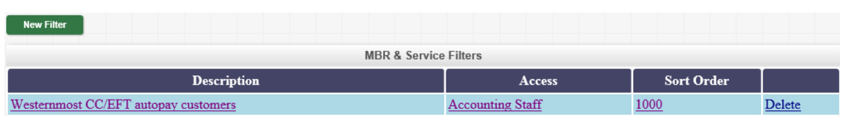
Global Default Fields

This menu enables configuration of field visibility options for Emerald client interface. See Field Visibility for more information.

Billing Group Fields

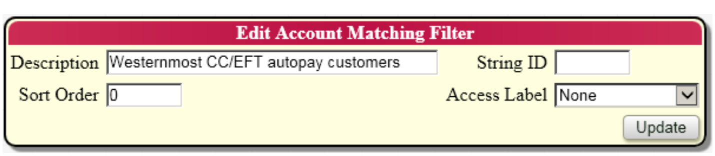
Per billing group level field visibility settings are configured from this menu. Note that only subset of fields that can be applied to a specific billing group are included. This generally includes any configurable fields within the MBR menu of an account. See Field Visibility for more information.

Account Filters



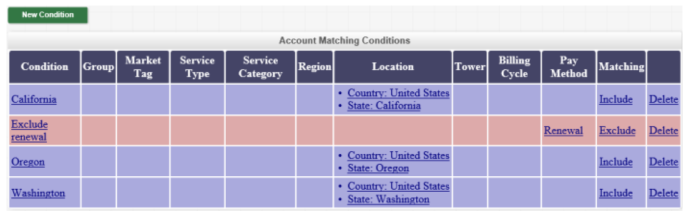
Account filters enable a series of inclusive and exclusive account parameters to define targeted customer lists. Account filters are currently used within support menu of Emerald client defining recipient list for bulk messaging feature and by events in order to determining those potentially affected by outages.

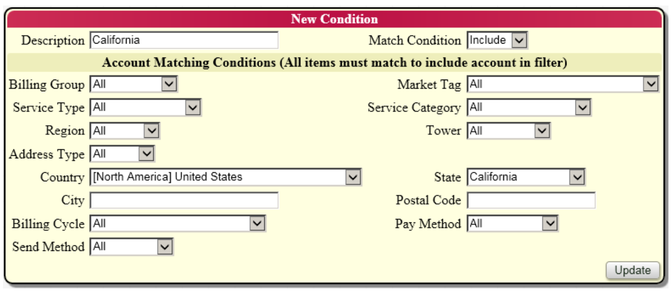
Any item within account filter having matching condition of "Include" adds to filter list of matching MBRs. If any items have a matching condition of "Exclude" then the matching MBRs are excluded from filter list.



Field	Description
Description	Unique name of account matching filter. Description appears as an option within bulk messaging and events areas of the Emerald Client / Support menu.
String ID	See Common fields
Sort Order	See Common fields
Access Label	See Common fields

Once a matching filter is created any number of inclusive and exclusive search parameters may be assigned to the filter.





<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Informational label detailing purpose of this match condition</td></tr>
<tr><td>Match Condition</td><td>Determines what occurs when matching condition is met.
<table><tr><th>Condition</th><th>Description</th></tr><tr><td>Include</td><td>When all matching conditions are met the MBR is included unless it also matches one or more exclude conditions.</td></tr><tr><td>Exclude</td><td>When all matching conditions are met the MBR is to be excluded regardless of whether the MBR matches one or more Inclusive conditions.</td></tr></table></td></tr>
<tr><td>Billing Group</td><td>If set MBR billing group must match selected group</td></tr>
<tr><td>Market Tag</td><td>If set MBR must have an active market tag of this type</td></tr>
<tr><td>Service Type</td><td>If set MBR must contain one or more active services having a matching service type</td></tr>
<tr><td>Service Category</td><td>If set MBR must contain one or more active services having a matching service category</td></tr>
<tr><td>Region</td><td>If set MBR region must have selected region</td></tr>
<tr><td>Tower</td><td>If set MBR must contain one or more active services assigned to the matching tower</td></tr>
<tr><td>Address Type</td><td>If Country, State, City or Postal Code is set address type restricts matching of these fields to addresses assigned to MBR having matching purpose.</td></tr>
<tr><td>Country</td><td>If set MBR must contain one or more addresses having a matching Country</td></tr>
<tr><td>State</td><td>If set MBR must contain one or more addresses having a matching State</td></tr>
<tr><td>City</td><td>If set MBR must contain one or more addresses having a matching City</td></tr>
<tr><td>Postal Code</td><td>If set MBR must contain one or more addresses having a matching Postal Code</td></tr>
<tr><td>Address Data Field</td><td>If set MBR must contain one or more addresses having a matching address data field and fields value must match value entered into Address Data field below</td></tr>
<tr><td>Address Data</td><td>See Address Data Field above. Required when address data field configured</td></tr>
</table>

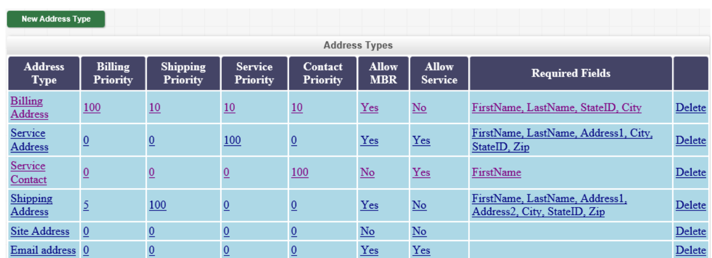
Billing Cycle	If set MBR billing cycle must match selected billing cycle
Payment Type	If set MBR pay method must match selected pay method
Send Method	If set MBR send method must match selected send method

GEOGRAPHY

Geography menu offers configuration of regions, address types, geocoding and geography.

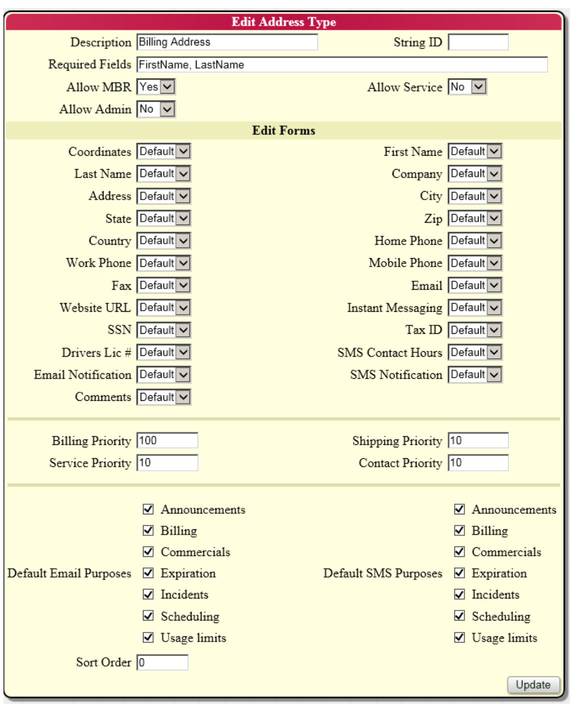
Address Types

Address Types define use and purpose of address information collected at the MBR and Service levels. Generally each address type depending on configured priority settings map to one or more of the following built-in uses: Billing Address, Shipping Address, Service Address and Contact Address.


New Address Type

Address Types

Address Type	Billing Priority	Shipping Priority	Service Priority	Contact Priority	Allow MBR	Allow Service	Required Fields	
Billing Address	100	10	10	10	Yes	No	FirstName, LastName, StateID, City	Delete
Service Address	0	0	100	0	Yes	Yes	FirstName, LastName, Address1, City, StateID, Zip	Delete
Service Contact	0	0	0	100	No	Yes	FirstName	Delete
Shipping Address	5	100	0	0	Yes	No	FirstName, LastName, Address1, Address2, City, StateID, Zip	Delete
Site Address	0	0	0	0	No	No		Delete
Email address	0	0	0	0	Yes	Yes		Delete

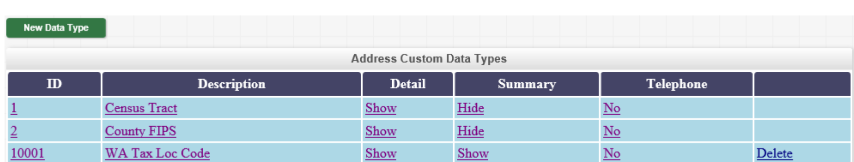


Field	Description
Description	Enter a description of the Address Type. This entry will be displayed as the label for the Address

	option on the MBR account Addresses entry screen.
String ID	See [Common fields]
Required Fields	A comma separated listing of required fields. The following field names are available to choose from: FirstName, LastName, PhoneHome, PhoneWork, PhoneFax, PhoneMobile, Email, WWW, SSN, TaxNumber, DLNumber, CountryID, StateID, Company, Address1, Address2, City, Zip, Lat, Long, Comments.
Allow MBR	Allows address type to be selected when creating an MBR or managing addresses assigned to MBR.
Allow Service	Allows address type to be selected when creating a service or managing addresses assigned to service.
Allow Admin	Allows the address type to be used to configure administrative addresses from Emerald Admin / General / Admin Addresses. Admin addresses are used for site & tower management and operator scheduling.
Billing Priority	Relative priority for addresses of this type to assume the role of primary billing address for the MBR. The address having an address type with the highest billing priority becomes the MBRs billing address. If there are multiple addresses of the same address type or multiple address types with the same billing priority the winning address is earliest address entered.
Shipping Priority	Relative priority for addresses of this type to assume the role of primary shipping address for the MBR. The address having an address type with the highest shipping priority becomes the MBRs shipping address. If there are multiple addresses of the same address type or multiple address types with the same billing priority the winning address is earliest address entered.
Service Priority	Relative priority for addresses of this type to assume the role of physical service location for the service. If an address is associated to a service and service priority is nonzero the service address takes precedence over any MBR assigned addresses even if the MBR address has an address type having a higher service priority. If service priority is zero then MBR address with highest service priority can be used for service address over service specific address.
Contact Priority	Relative priority for addresses of this type to assume the role of contact address for the service. Contact is generally the primary user of the account. If there are no service specific addresses associated with a service the MBR level address with highest contact priority is used otherwise MBR billing address is used if there is no MBR level address with a contact priority above 0. If there are one or more addresses assigned to service then the address having an address type with the highest non-zero contact priority becomes the services contact address. If there are multiple addresses of the same address type or multiple address types with the same contact priority the winning address is earliest candidate address entered.
Default Email and SMS Purposes	Sets address type specific defaults for reasons the address should be contacted with information relative to checked purposes. If 'Email Notification' and or 'SMS Notification' edit forms field visibility is enabled the default purposes can be customized when entering address. Purposes are recorded stored with each address. The defaults apply only during creation of new addresses. Changes to default Email or SMS purpose settings at the address type level have no effect on existing addresses.
Sort Order	See [Common fields]

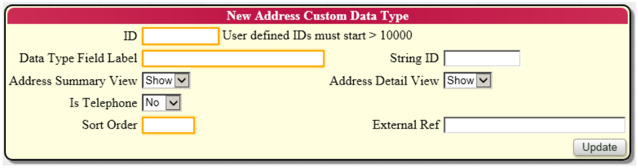
Address Data Types

Address Data Types enable additional custom data fields to be assigned to MBR and Service addresses enabling extra address related data to be stored and



ID	Description	Detail	Summary	Telephone	
1	Census Tract	Show	Hide	No	
2	County FIPS	Show	Hide	No	
10001	WA Tax Loc Code	Show	Show	No	Delete

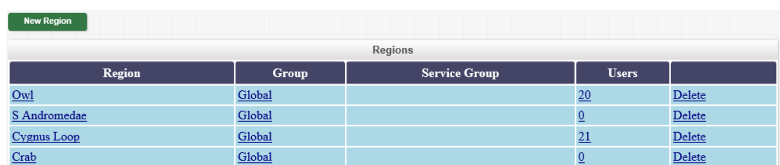
displayed with the address. These new data fields can be populated manually by assigning fields to an Address Type or they can be populated automatically by synchronization with geographic layers.



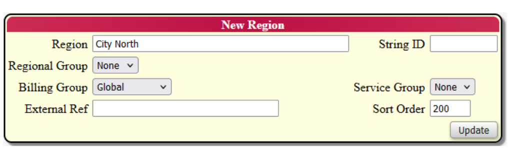
Field	Description
ID	Unique number assigned to the address data type. When creating a new address data type it is important to choose an unused ID number greater than 10000 to prevent custom data field from being modified by future software updates.
Data Type Field Label	Label describing custom data field
String ID	Supports localization of "Data Type Field Label". See Common fields
Allow Summary View	When 'Yes' data field is displayed with address information within Show MBR/Show Service menus if address contains a value for this custom data field. When 'No' data field is hidden from the Show MBR/Show service menus.
Allow Detail View	When 'Yes' data field is displayed when making changes to an address.
Is Telephone	When 'Yes' the custom data field is treated as a phone number for search and presentation purposes.
Access Label	See Common fields
Sort Order	See Common fields
External Ref	See Common fields

Regions

Regions generally represent distinct geographical areas where your organization offers service but they are not limited to this purpose and may be used to facilitate logical grouping of



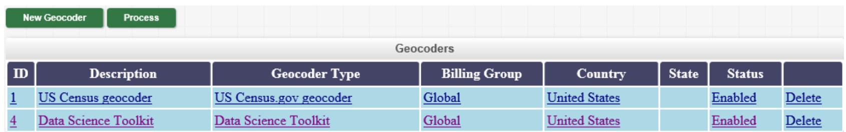
accounts for reporting purposes. Regions may also influence taxes assigned to accounts (See Tax Groups) and are used primarily for reporting, grouping or external integration purposes.



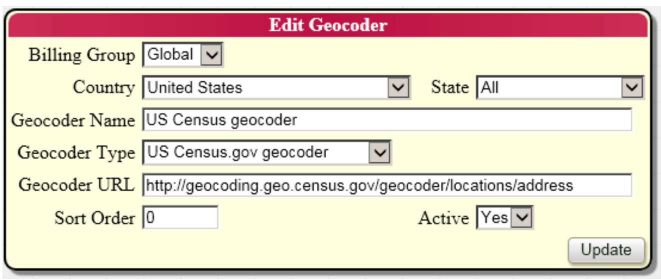
Field	Description
Region	Choose a descriptive name for the Region. This name appears when selecting a region from the edit MBR menu within Emerald client.
String ID	See Common fields
Regional Group	Organize related regions together for improved organization and reporting when large numbers of regions are used. Once one or more regions have been linked to a regional group they are grouped together under a common group heading within region selection lists throughout the Emerald UI. Available regional groups are managed from Region Groups menu.

Billing Group	See Common fields
Service Group	See Common fields
External Ref	See Common fields
Sort Order	See Common fields

Geocoders



Geocoder services determine latitude and longitude of a customer location based on account address information. Once geographic coordinates are known for an address then it becomes usable for service tower selection, onsite scheduling and geographic queries to obtain information related to market, service area, taxation and regulatory reporting.



Support for many popular geocoding services is included. Some services are free to use while others require creation of an account and payment for commercial use. Multiple geocoder services may be used concurrently to improve automatic conversion rate or reduce costs. To enable click New Geocoder from Emerald Admin / Geography / Geocoders menu.

Field	Description
Billing Group	Restricts geocoding to addresses associated with chosen billing group
Country	Restricts geocoding to address with matching country
State	Restricts geocoding to addresses with matching state of selected country
Geocoder Name	Description of geocoder
Geocoder Type	List of supported geocoding services
Geocoder URL	URL for submitting geocoding requests
*** (Geocoder Specific)	Geocoder types requiring authentication or additional settings are shown here. For information about additional configuration fields please check vendor documentation corresponding to selected geocoder type.
Sort Order	If multiple geocoders are enabled they are executed in order of applicable geocoders starting from the lowest sort order to highest. This can be useful to give lower cost geocoders a first opportunity to locate an address before moving to higher cost services.

Geocoding is performed when adding a new MBR and also periodically when an address has been changed or added and the geoexport task is activated from Emerald / Admin / Scheduler / Configure Schedules. Geocoding can also be processed manually for a geocoder by clicking "Process" option in Geocoder list once a geocoder has been configured.

```
To ensure coordinates associated with new or changed address are kept current check to confirm "Geocode accounts with new or updated address information" scheduled task is activate from Emerald Admin / Scheduler / Configure schedules menu.
```

Layers

Collections of areas drawn on a map annotated with data or labels describing drawn area are organized into "layers" available to be used by Emerald for reporting or assigning of address custom data fields to accounts. An example of a layer is a list of cities where geographic boundaries of each city is annotated with data such as city name, population, region, national identifier and tax rate.

Geographic Layers

ID	Layer Name	Create Date	Status	Data Fields	Sublayers	Shapes	
11	ID Tax Code Areas	02/11/19 16:23:36	Valid	• tKey • TCANUM • COUNTY • AlignID	0	6571	Delete
6	US Census Place	10/31/18 22:06:10	Valid	• PLACENS • GEOID • LSAD • NAME • NAMELSAD	1	626	Delete
2	US Census Tract	02/21/17 13:03:17	Valid	• TRACTCE • COUNTYFP	1	1458	Delete
5	US Counties	10/31/18 22:16:59	Valid	• COUNTYNS • GEOID • NAME • NAMELSAD	0	3233	Delete
7	WA Tax Locations	02/06/19 16:01:32	Valid	• LOCCODE	0	355	Delete
1	WA Tax Rates	10/31/18 22:04:16	Valid	• Rate • CITY_DISSO • CITY • PLACE	0	431	Delete

Layers are imported into Emerald using the geoimport command line tool located in the Emerald folder. To use geoimport from command line type geoimport followed by name of the ".geo" files to import. Geo files are typically created by processing standard ESRI shapefiles using IEA shapefile conversion tool. Shapefiles can be generated by any GIS system and are commonly available from countrywide and state governments. Converted ".geo" files of general interest to service providers are also available from the IEA Software website.

Once a layer has been successfully loaded its status appears as "Valid" in layer list. If for any reason a layer does not load successfully geoimport tool displays a failure reason and partially loaded layers appear with status of 'Invalid'. Partially loaded layers can either be deleted from the UI or the geoimport tool rerun to reattempt complete loading of the layer.

When reloading an updated version of the same dataset simply run geoimport utility for new file and existing layer will automatically be updated. Once updated any address data syncs associated with updated layer are automatically refreshed the next time address data is processed.

When layers are used it is generally also necessary to enable Geocoders to obtain geographic coordinates of customer and administrative addresses.

Address Layer Data

Address layer data facilitates synchronization of geographic datasets contained in layers with address data fields based on geographic coordinates of MBR and Service level addresses. Once data has been synchronized it may be used for purposes including reporting, tax rate determination and market tag activation.

New Layer Match

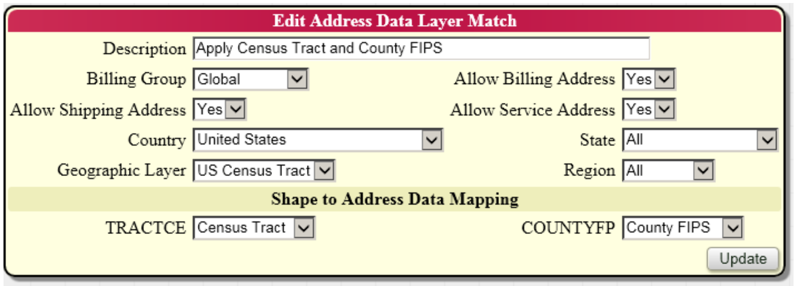
Geographic Layer Matching for Address Data

Description	Layer	Shape Data Mapping	Applies To	Group	Country	State	Region	
FCC form 477	US Census Tract	• TRACTCE: Census Tract • COUNTYFP: County FIPS	• Service Address	Global	United States	All	All	Delete
WA Tax Location Code	WA Tax Locations	• LOCCODE: WA Tax Loc Code	• Billing Address • Shipping Address • Service Address	Global	United States	Washington	All	Delete

Before this feature can be used the following prerequisites are necessary:

- Geographic coordinates must be obtained for MBR and Service level addresses. Latitude / Longitude coordinates may be entered for each address manually or obtained automatically by enabling one or more Geocoders.

- Layers containing geographic dataset to be queried and synchronized must be loaded using geoimport tool.
- Address Data Types to define address custom data fields where synchronized geographic data is to be stored must be configured.

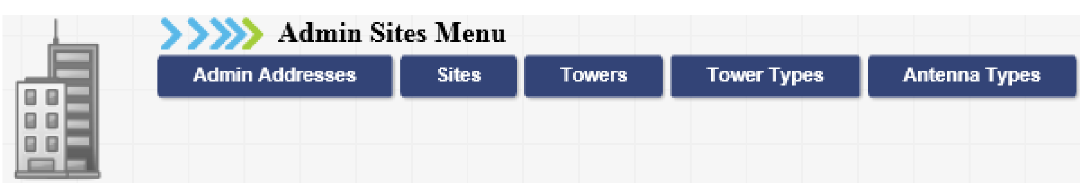


Field	Description
Description	Shor text explaining the purpose of the synchronization
Billing Group	When configured address data synchronization is only performed for addresses belonging to the configured billing group.
Allow Billing Address	Allow synchronization for addresses assigned as the MBR billing address
Allow Shipping Address	Allow synchronization for addresses assigned as the MBR shipping address
Allow Service Address	Allow synchronization for addresses assigned as service level service address
Country	When configured synchronization is limited to addresses within selected country
State	When configured synchronization is limited to addresses within selected state
Geographic Layer	Selection of layer containing geographic dataset to be synchronized with MBR and Service level addresses. Once a layer is selected the form is automatically updated with address data mapping options specific to selected layer.
Region	When configured synchronization is limited to addresses within selected region
*** (Shape to Address Data Mapping)	Each field displayed represents a column of the geographic dataset of the selected geographic layer. If data contained within a field of the layer is to be synchronized with a MBR or Service level address select the corresponding address data type where data is to be stored from the selection list.

> By default synchronization occurs four times daily from the scheduled task "Geographic match address coordinates by layer". Synchronization can also be executed manually at any time by clicking "Process Address Data" menu option.

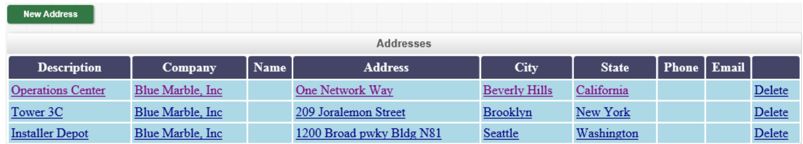
SITES

Sites menu offers configuration of site locations and towers supporting reporting, inventory, scheduling and fixed wireless management.



Admin Addresses

Admin addresses define locations relevant to your organization such as business offices and network facilities. For configuration of administrative address types and field availability see Address Types.



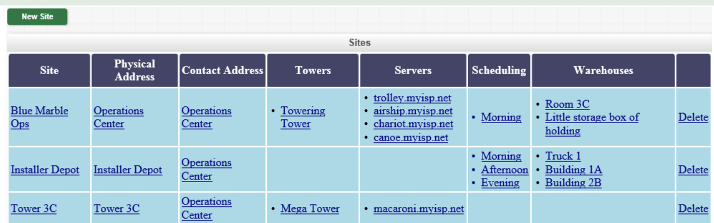
New Address

Addresses

Description	Company	Name	Address	City	State	Phone	Email	
Operations Center	Blue Marble, Inc		One Network Way	Beverly Hills	California			Delete
Tower 3C	Blue Marble, Inc		209 Joralemon Street	Brooklyn	New York			Delete
Installer Depot	Blue Marble, Inc		1200 Broad pwky Bldg N81	Seattle	Washington			Delete

Sites

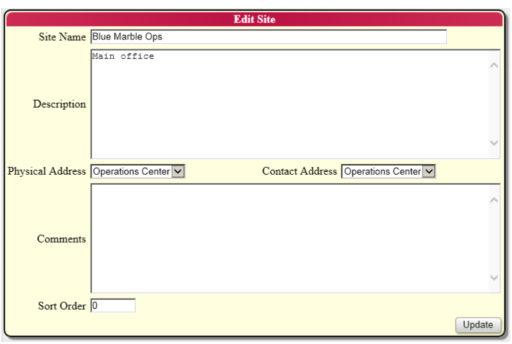
Sites define locations and contacts used by your organization to provide service. Sites may be used by access servers, tower management, inventory and appointment scheduling for reporting and location based features.



New Site

Sites

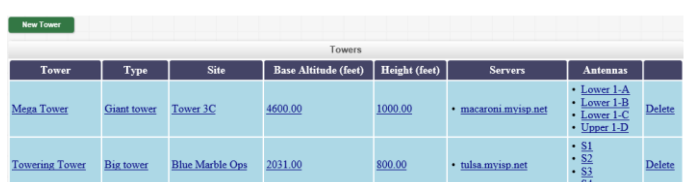
Site	Physical Address	Contact Address	Towers	Servers	Scheduling	Warehouses	
Blue Marble Ops	Operations Center	Operations Center	• Towering Tower	• trolley.myisp.net • airship.myisp.net • chariot.myisp.net • canoe.myisp.net	• Morning	• Room 3C • Little storage box of holding	Delete
Installer Depot	Installer Depot	Operations Center			• Morning • Afternoon • Evening	• Truck 1 • Building 1A • Building 2B	Delete
Tower 3C	Tower 3C	Operations Center	• Mega Tower	• macaroni.myisp.net			Delete



Field	Description
Site Name	Unique label describing the site. Site name appears in selection lists when choosing a site throughout Emerald.
Description	Additional details describing the site
Physical Address	Admin address representing physical location of the site
Contact Address	Admin address representing who to contact for inquiries related to the site
Comments	Additional information
Sort Order	See Common fields

Towers

This menu offers service tower selection and qualification for fixed wireless broadband and reporting. Configuration includes management of tower characteristics including location, size and

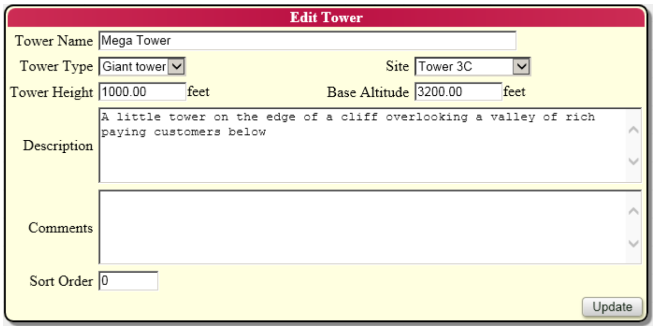


New Tower

Towers

Tower	Type	Site	Base Altitude (feet)	Height (feet)	Servers	Antennas	
Mega Tower	Giant tower	Tower 3C	4600.00	1000.00	• macaroni.myisp.net	• Lower 1-A • Lower 1-B • Lower 1-C • Upper 1-D	Delete
Towering Tower	Big tower	Blue Marble Ops	2031.00	800.00	• tulsa.myisp.net	• S1 • S2 • S3 • S4	Delete

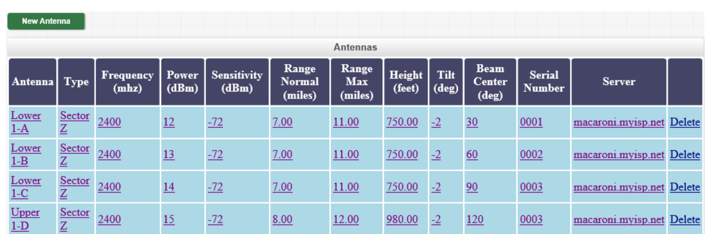
tower type as well as associated antennas, radios and services.



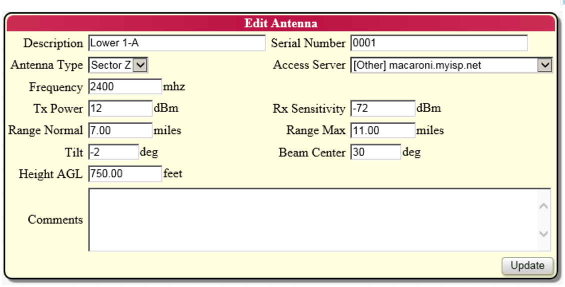
Field	Description
Tower Name	Display name for tower used in service tower selection tool as well as tower related reporting
Tower Type	Normally a selection of style or structural type used for informational and reporting purposes. See Tower Types.
Site	Defines physical location of tower. See Sites.
Tower Height	Total height of tower above ground level
Base Altitude	Altitude above sea level of tower base. If not configured elevation heightmap will be used when available to determine altitude in service tower selector.
Description	Additional information describing tower
Comments	Related comments
Sort Order	See Common fields

Tower Antennas

Once a tower has been configured antennas may be assigned to the tower defining antenna type, position and estimated range. This information is used for tower service selection and reporting.



Antenna	Type	Frequency (mhz)	Power (dBm)	Sensitivity (dBm)	Range Normal (miles)	Range Max (miles)	Height (feet)	Tilt (deg)	Beam Center (deg)	Serial Number	Server	
Lower 1-A	Sector Z	2400	12	-72	7.00	11.00	750.00	-2	30	0001	macaroni.myisp.net	Delete
Lower 1-B	Sector Z	2400	13	-72	7.00	11.00	750.00	-2	60	0002	macaroni.myisp.net	Delete
Lower 1-C	Sector Z	2400	14	-72	7.00	11.00	750.00	-2	90	0003	macaroni.myisp.net	Delete
Upper 1-D	Sector Z	2400	15	-72	8.00	12.00	980.00	-2	120	0003	macaroni.myisp.net	Delete



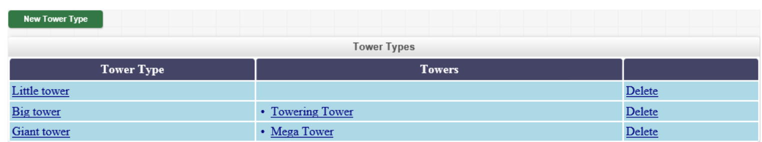
Field	Description
Description	Label which uniquely describes antenna for this tower
Serial Number	Serial number associated with antenna hardware
Antenna Type	Determines antenna characteristics such as gain and beam width. See Antenna Types
Access Server	Selection of access server / radio used by antenna. Currently used only for reporting purposes.

Frequency	Lowest frequency in megahertz to be transmitted or received from this antenna. This is required for path loss calculation.
Channel Width	Bandwidth of communications channel in mhz. This field is informational and not used in calculating path loss.
Tx Power	Maximum transmit power in dBm. When entering power subtract known sources of transmission losses such as cabling and connectors. Required for calculating signal level as received by service.
Rx Sensitivity	Receive sensitivity in dBm. Required for calculating link margin within service path profile of service tower selector.
Range Normal	Normal expected range from antenna where service is expected to be provided normally.
Range Max	Maximum range from antenna where service is expected to be provided perhaps with some restrictions such as limited service tier or special customer premise equipment requirements.
Tilt	Vertical tilt of antenna in degrees. Positive value represents an upward tilt and negative value a downward tilt.
Beam Center	Degrees from true north representing direction antenna is pointing
Height AGL	Height of antenna as measured from base of tower. This is required for path loss calculation.
Comments	Related comments

Once an antenna is configured one or more service categories can be assigned to the antenna representing services provided by this antenna. This information is used by the service tower selector and reporting purposes.

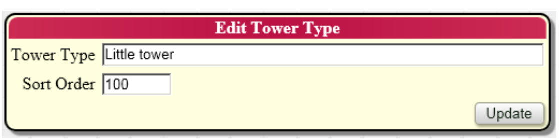
Tower Types

Types offer an option to classify types of tower in use by structural type or other characteristics as needed.


New Tower Type

Tower Types

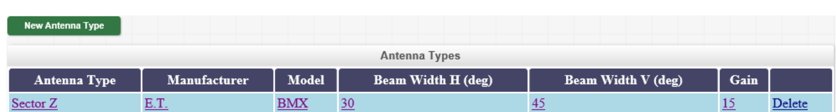
Tower Type	Towers	
Little tower		Delete
Big tower	• Towering Tower	Delete
Giant tower	• Mega Tower	Delete



Field	Description
Tower Type	Label uniquely describing tower type. Shown in tower type selection field when adding or updating a tower.
Sort Order	See Common fields

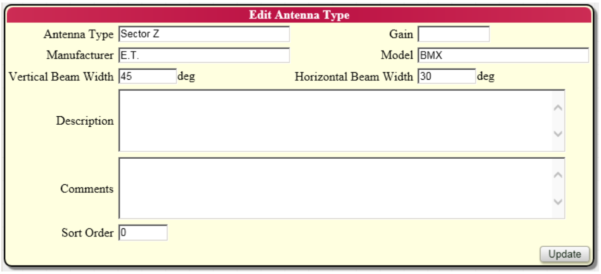
Antenna Types

Antenna types provide information about characteristics of antennas assigned to towers. Antenna types are used for service tower selection and reporting.


New Antenna Type

Antenna Types

Antenna Type	Manufacturer	Model	Beam Width H (deg)	Beam Width V (deg)	Gain	
Sector Z	E.T.	BMX	30	45	15	Delete



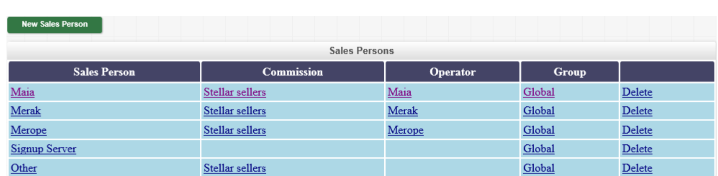
Field	Description
Antenna Type	Unique label describing the antenna
Gain	Antenna gain in dB. Required for calculating signal level as received by service.
Manufacturer	Manufacturer
Model	Model number
Vertical Beam Width	Vertical beam width in degrees
Horizontal Beam Width	Horizontal beam width in degrees. Used by service tower selector.
Description	Additional details
Comments	Related comments
Sort Order	See Common fields

SALES & MARKETING

Sales menu offers configuration of sales persons, commissions and referrals as well as market related configuration of discounts, promotional codes and market tags.

Sales Persons

Sales Persons are assignable to MBRs and services for purposes of commission tracking and reporting. If sales person is associated with an operator then the corresponding sales person is set as the default sales person whenever the associated operator creates a new service.

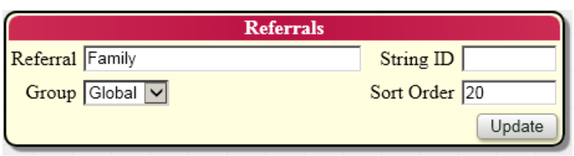


Field	Description
Sales Person	Enter a description of the Referral source. This description will be used within the Emerald "Sales Person" selection pick lists.
Operator	Provides for the association of Emerald Operators to sales persons for future reporting purposes.
Commission	A commission structure if any that should be applied to this sales person. When a commission is selected the commission report will begin to provide sales commission data for the sales person. See "Commissions" for more information on configuring commissions.
Commission Multiplier	Serves as a point multiplier of points configured in the selected commission. If left blank a value of 1 is assumed as the commission's multiplier.
Billing Group	See Common fields
Service Group	See Common fields
Sort Order	See Common fields

Referred By

Referrals can offer insights into how customers are hearing about your organization and services. Referrals are selected at the MBR level when adding or updating an MBR. Referrals are exclusively informational for reporting purposes only.

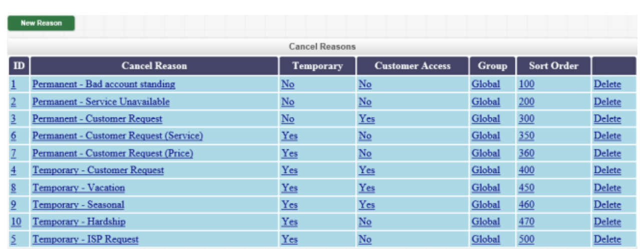
Referral	Group	Sort Order	
Friend	Global	10	Delete
Family	Global	20	Delete
Advertising	Global	30	Delete
Website	Global	40	Delete
Search Engine	Global	50	Delete
Other	Global	100	Delete



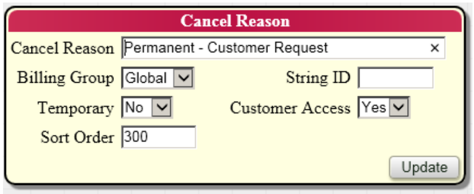
Field	Description
Referral	Enter a description of the Referral source. This description will be used within the Emerald 'Referred By' selection pick lists.
Group	See Common fields
String ID	See Common fields
Sort Order	See Common fields

Cancel Reasons

Cancel reasons indicate reason for closing an MBR or service and may be either permanent where account is not expected to be reopened or temporary where service is likely to be resumed in the future. Closing an MBR or service with a Cancel reason not marked temporary can trigger automatic assessment of ETF fees if configured within Market Tags.

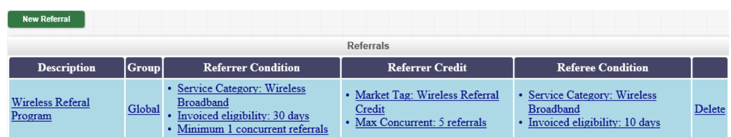


ID	Cancel Reason	Temporary	Customer Access	Group	Sort Order	
1	Permanent - Bad account standing	No	No	Global	100	Delete
2	Permanent - Service Unavailable	No	No	Global	200	Delete
3	Permanent - Customer Request	No	Yes	Global	300	Delete
6	Permanent - Customer Request (Service)	Yes	No	Global	350	Delete
7	Permanent - Customer Request (Price)	Yes	No	Global	360	Delete
4	Temporary - Customer Request	Yes	Yes	Global	400	Delete
8	Temporary - Vacation	Yes	Yes	Global	450	Delete
9	Temporary - Seasonal	Yes	Yes	Global	460	Delete
10	Temporary - Hardship	Yes	No	Global	470	Delete
5	Temporary - ISP Request	Yes	No	Global	500	Delete



Field	Description
Cancel Reason	Choose a descriptive cancellation reason. This description will be used within the Emerald 'Cancel Reasons' selection list when closing an MBR or Service.
Billing Group	See Common fields
Temporary	If the cancel reason is expected to be temporary with a reasonable chance the MBR or service will be reopened in the future temporary should be set "Yes". If MBR or service is unlikely to be resumed in the future temporary should be set "No". This setting controls availability of reopen date prompt and affects assessment of ETF fees if configured within a Market Tag.
Customer Access	When Customer Access is enabled and the customer is allowed to cancel their services from the customer interface this cancel reason is made available for the customer to choose.
String ID	See Common fields
Sort Order	See Common fields

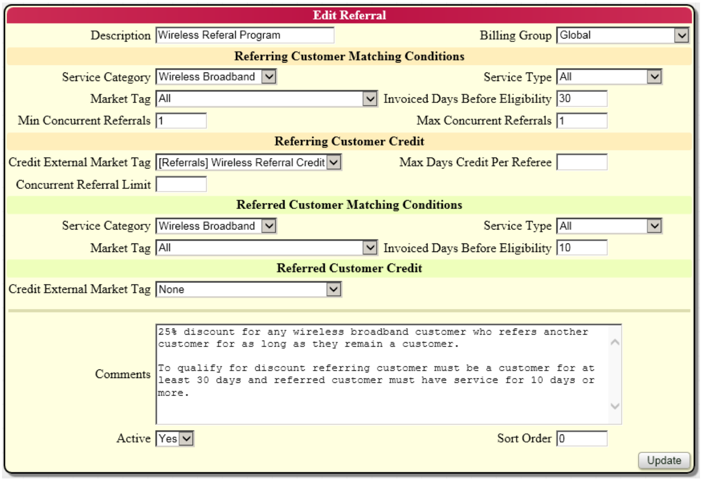
Referral Manager



To incentivize existing customers to refer new customers referral manager provides for automated assessment of referral benefits. Referrals may be time limited such as benefits covering first three months or they may continue for as long as the referred customer remains an active subscriber. Benefits may be tiered to provide escalating reward incentives for customers who successfully refer more and more business.

Assessment of benefits to the referring and optionally referred party is facilitated by referral manager taking automatic action to activate and refill service level externally assigned market tags. Tags in-turn are able to directly or indirectly offer discounts on recurring subscription costs and or modify RADIUS authorization to for example affect bandwidth allocation.

It should be noted all tracking of benefits is based on an invoiced view of service regardless of payment status. While retroactive changes such as account cancellation are accounted for and reflected in future invoicing activity credits already applied to a generated invoice are not retroactively removed unless the account is manually reinvoiced. To mitigate liability and referral fraud "Invoiced Days before Eligibility" setting may be used to enable a probationary period to pass before assessment of referral benefits begin.

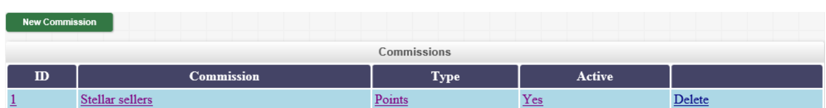


Reference	Field	Description
N/A	Description	Unique label detailing purpose of referral
N/A	Billing Group	If set the referral is restricted to accounts with matching billing group
Referring	Service Category	If set referring service must be associated with selected service category
Referring	Service Type	If set referring service must be associated with selected service type
Referring	Market Tag	If set referring service must have a matching active service level market tag.
Referring	Invoiced Days Before Eligibility	Number of days the referring service must have been invoiced before referral is applicable.
Referring	Min Concurrent Referrals	Minimum number of concurrently active referrals of this type needed for referring customer credit to be applicable.
Referring	Max Concurrent Referrals	Maximum number of concurrently active referrals of this type after which the referring customer credit is not applicable. This setting combined with min concurrent referrals enables a series of referrals to be configured in order to offer graduated referral credits based on total number of active referred customers.
Referring	Credit External Market Tag	While all conditions have been met the selected service level external market tag is activated and invoiced days allowance updated as necessary to reflect continuing applicability of referral credit. Normally the selected external market tag will either directly or indirectly be assigned a discount for purposes of reducing referring customers normal recurring service cost. The selected external market tag must be configured with "Allow Invoiced Days Max" set "Yes" in order to enforce restricting external tag applicability to quantity of "invoiced days" transferred to this tag by referral manager.
Referring	Max Days credit per Referee	Defines an upper limit to number of days a referral can be applicable per referred customer. For example in a scenario where referring customer gets a 25% service discount for the first 6 months per referred customer this would be set to 180 days (30 days * 6 months). Every month is counted as 30 days for the purposes of configuration. In a situation where the referring customer retains the referral credit as long as referred customer remains this field should be left blank to indicate no limit.
Referring	Concurrent referral limit	In the case where referring customer has multiple active referrals this sets a ceiling on the number of referrals that may concurrently contribute to the referring services credit. Any excess referrals are ignored.
Referred	Service Category	If set referred service must be associated with selected service category

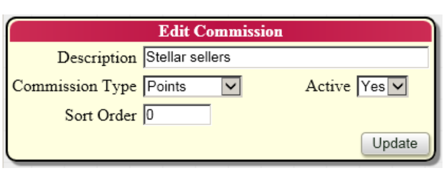
Referred	Service Type	If set referred service must be associated with selected service type
Referred	Market Tag	If set referred service must have a matching active service level market tag.
Referred	Invoiced Days Before Eligibility	Number of days the referred service must have been invoiced before referral is applicable.
Referred	Credit External Market Tag	While all conditions have been met the selected service level external market tag is activated and invoiced days allowance updated as necessary to reflecting continuing applicability of referred credit. Normally the selected external market tag will either directly or indirectly be assigned a discount for purposes of reducing referred customers normal recurring service cost. The selected external market tag must be configured with "Allow Invoiced Days Max" set "Yes" in order to enforce restricting external tag applicability to quantity of "invoiced days" transferred to this tag by referral manager.
N/A	Comments	Normally used to write a detailed description of what the referral is to do.
N/A	Active	When "Yes" the referral is active and matches are allowed to continue to credit external market tag. When "No" the referral is inactive and no new day credits are assigned however this does not affect existing invoiced days previously allocated to credit external market tags.
N/A	Sort Order	See Common fields

```
Referral manager requires scheduled task "Process customer referrals" enabled
from Configure Schedules menu of Emerald scheduler.
```

Commissions

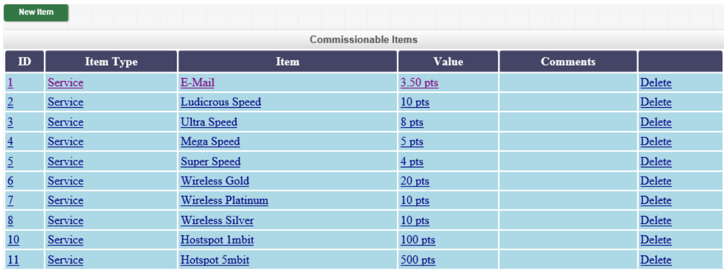


Basic commission reporting enables sales staff to be awarded credit for sale of one time and recurring products and services. Each sales person to be included in commission reporting is assigned to a commission where credit in percentage or point basis by service type and charge type is determined. Commission reporting offers sales reporting both in terms of items invoiced and items paid by sales person.



Field	Description
Description	Text describing purpose and use of the commission.
Commission Type	Controls whether commissions are based on either a percentage of the amount invoiced or a set number of points for each item invoiced.
Active	When active the commission is visible to the commission report
Sort Order	See Common fields

Once a commission is created service types and charge types subject to commission are assigned to the commission.

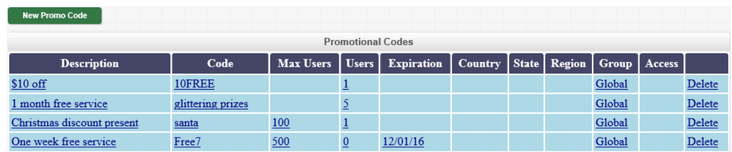

New Item

Commissionable Items

ID	Item Type	Item	Value	Comments	
1	Service	E-Mail	3.50 pts		Delete
2	Service	Ludicrous Speed	10 pts		Delete
3	Service	Ultra Speed	8 pts		Delete
4	Service	Mega Speed	5 pts		Delete
5	Service	Super Speed	4 pts		Delete
6	Service	Wireless Gold	20 pts		Delete
7	Service	Wireless Platinum	10 pts		Delete
8	Service	Wireless Silver	10 pts		Delete
10	Service	Hostspot 1mbit	100 pts		Delete
11	Service	Hotspot 5mbit	500 pts		Delete

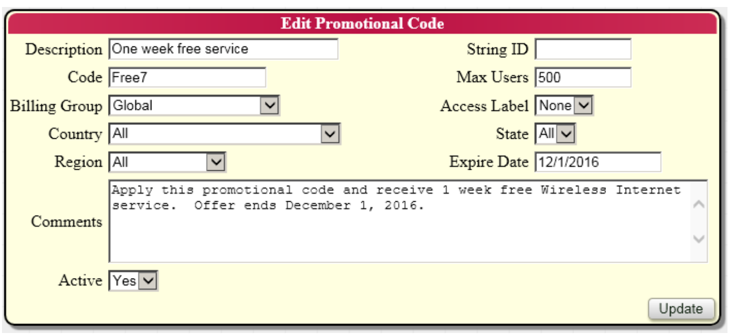
Promo Codes

Promotional codes may be assigned to MBRs by operators within Emerald client or by customers during customer self-signup or within customer account center. Once a promo code has been assigned to an MBR it is available to satisfy promo code matching condition of a market tag to effect temporary or permanent service discounting and other account related changes.


New Promo Code

Promotional Codes

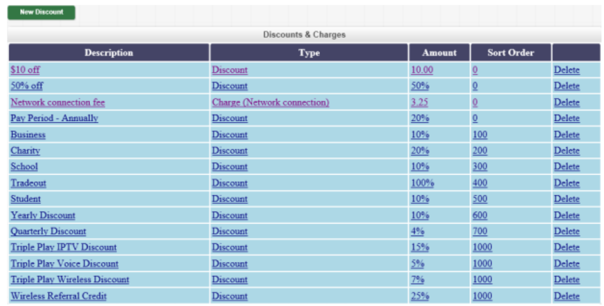
Description	Code	Max Users	Users	Expiration	Country	State	Region	Group	Access	
$10 off	10FREE		1					Global		Delete
1 month free service	glittering prizes		5					Global		Delete
Christmas discount present	santa	100	1					Global		Delete
One week free service	Free7	500	0	12/01/16				Global		Delete

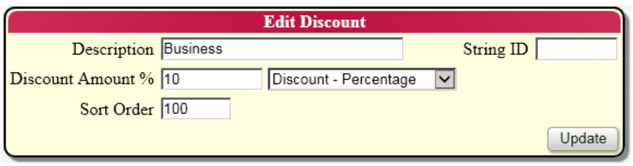


Field	Description
Description	Unique label for this promotion code
String ID	See Common fields
Code	Promotion code to be entered by customer when applying code to MBR
Max Users	Maximum number of customers allowed to use this code before it is no longer available
Billing Group	If set promotion code may only be applied to MBRs within selected billing group
Access Label	See Common fields
Country	If set promotion code may only be applied to MBRs having billing address within selected country.
State	If set promotion code may only be applied to MBRs having billing address within selected state.
Region	If set promotion code may only be applied to MBRs having matching region
Expire Date	Date after which the promotion code may no longer be applied to an MBR. Expiration date does not affect existing MBRs where the promo code has already been applied.
Comments	Additional details describing use and benefits of this promotion code
Active	When "Yes" promotion code is available to be applied to an MBR. When "No" the promotion code may not be applied to an MBR. The active status of promotion code does not affect existing MBRs where promo code has already been activated.

Discounts

Discounting enables percentage basis or static amount reduction to be applied to recurring services via matched tag area of service level market tags. Regardless of percentage or static amount aggregate effect of all applicable discounts on a service shall never result in a service with a negative (credit) price. Discounting is often used to customize reductions in pricing based on criteria such as customer type, double and triple play, quarterly or yearly prepayment, promotional, loyalty and regional/market based pricing.





<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Enter the identifying name for the Discount. This description will be used within the ‘Discount’ selection pick lists throughout Emerald.</td></tr>
<tr><td>String ID</td><td>See Common fields</td></tr>
<tr><td>Amount</td><td>The discount or charge amount as a static amount of percentage of service cost per table below.

<table>
<tr><th>Amount Type</th><th>Description</th></tr>
<tr><td>Discount - Percentage</td><td>Amount is a discount expressed as percentage of service cost. Discount percentage must not exceed 100.

Negative discounts are allowed to increase the service cost. For example -100 doubles service cost.</td></tr>
<tr><td>Discount - Static</td><td>Amount is a discount expressed in applicable currency independent of service cost. If discount amount exceeds service cost the service cost remains at zero and cannot become negative.

Negative discounts are allowed to increase the service cost for example -10 increases the charge or monthly service cost by 10.</td></tr>
<tr><td>Charge - Percentage</td><td>Amount is applied as a separate charge line item with cost derived as percentage of service cost. Amount must be a non-zero positive value. Charge percentage may exceed 100.</td></tr>
<tr><td>Charge - Static</td><td>Amount is applied as a separate charge line item of a given monthly or per charge cost. Amount must be a non-zero positive value.

Static charges are still applicable when the underlying charge or monthly service cost is 0. If the applied charge line item is itself subject to discounting then only discount percentage or static are applicable. Charge percentage and charge static if applicable are ignored in this case and shall not be applied recursively.</td></tr>
</table>
</td></tr>
</table>

	In the event multiple discounts are applicable to a service discounts are applied in the order of market tag sort order with each discount affected by changes to cost from preceding discounts.
Charge Type	When amount type is a Charge this mandatory field determines line item description, GL categorization and tax group assignment of the charge.
Sort Order	See Common fields

Market Tags

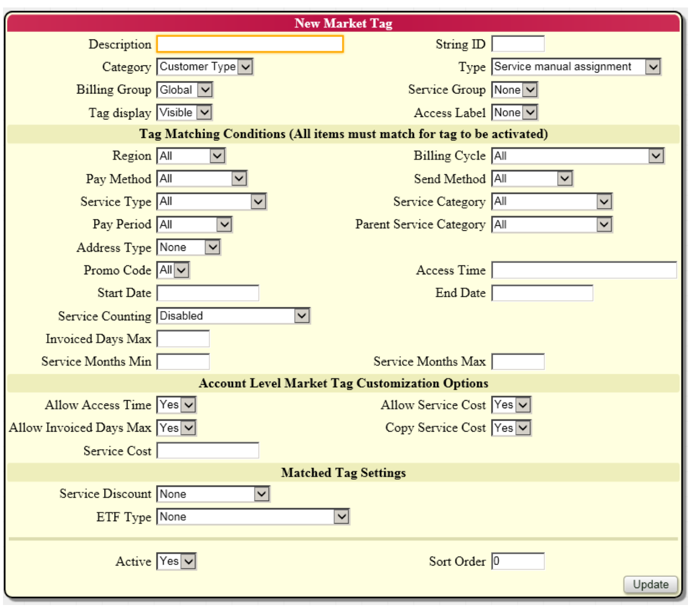
Tags represent facts about MBRs or services derived manually from operator selection or automatically based on match of MBR or service specific information. Examples of Market tags include VIP, business, school, charity, service length/loyalty, location, double and triple play.

Tags may be entirely informational simply to organize and report on accounts with similar properties. Alternately tags can affect pricing by applying discounts, static pricing, ETF charges and modifying RADIUS authorization attributes.

During invoicing tags are constantly evaluated for applicability over term of the invoice. Price affecting changes not constant throughout invoice term causes line items to be automatically split to account for any changes. For example if a service is invoiced for a full year's service with an introductory discount for the first three months of service the invoice line item for 12 months of service is broken into two separate line items: first 3 months with introductory discount applied followed by remaining 9 months at the normal rate.

Automatic market tags can be configured to depend on or conflict with other tags. Examples include "promotional discounts are incompatible with pay period discounts" or "business loyalty discount requires both business tag and 1 year of service tag".

Each service has access to MBR level tags as well as service level tags related to it. Services cannot directly access service level tags of other services within the same MBR. For this reason any tags with dependencies on status of other services within an account must be selected from MBR level tags.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Description shown when selecting or viewing tags</td></tr>
<tr><td>StringID</td><td>Provides localized version of Description field above. See Common fields for details.</td></tr>
<tr><td>Category</td><td>Offers grouping of related tags</td></tr>
<tr><td>Type</td><td>Determines level (MBR or Service) and method of assignment (auto, manual, external) the tag will have. Only automatically assigned tags may have tag matching conditions to depend or conflict with other tags assigned to them.

<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>MBR manual assignment</td><td>Tag is available to be enabled at the MBR level manually from the MBRs Market Tag menu.</td></tr>
<tr><td>MBR auto assignment</td><td>Tag will automatically be enabled at the MBR level if all of the tags matching conditions and dependencies are met.</td></tr>
<tr><td>MBR externally assigned</td><td>MBR level tag will be enabled or disabled managed by an external process</td></tr>
<tr><td>Service manual assignment</td><td>Tag is available to be enabled at the Service level manually from the Services Market Tag menu.</td></tr>
<tr><td>Service auto assignment</td><td>Tag will automatically be enabled at the Service level if all of the tags matching conditions and dependencies are met.</td></tr>
<tr><td>Service externally assigned</td><td>Service level tag will be enabled or disabled managed by an external process</td></tr>
<tr><td>Charge Type auto assignment</td><td>Tag will automatically be enabled at level of charge adjustments as they are rolled into invoices enabling discounting of charges.</td></tr>
</table></td></tr>
<tr><td>Billing Group</td><td>If configured tag shall be available only to MBRs with matching billing groups</td></tr>
<tr><td>Service Group</td><td>If configured tag shall be available to MBRs of billing groups associated with the selected service group in addition to MBRs matching billing group setting configured above.</td></tr>
<tr><td>Operator Display</td><td>Controls visibility of market tag in Show MBR and Show service displays. When hidden tag is not shown even while active. Useful for tags used primarily for abstraction and backend purposes which may have limited utility in being displayed.</td></tr>
<tr><td>Customer Display</td><td>Controls visibility of currently active MBR and Service level market tags from within manage accounts area of customer account center. When hidden tag is not displayed in customer account center.</td></tr>
<tr><td>Access Label</td><td>Limits activation or deactivation of manually assigned market tags to operators authorized for selected access label.</td></tr>
<tr><td>Region</td><td>If configured tag can only be active within accounts where the MBR’s region matches configured region.</td></tr>
<tr><td>Billing Cycle</td><td>If configured tag can only be active within accounts where the MBR’s billing cycle matches configured billing cycle.</td></tr>
<tr><td>Pay Method</td><td>If configured tag can only be active within accounts where the MBR’s pay method matches configured pay method.</td></tr>
<tr><td>Send Method</td><td>If configured tag can only be active within accounts where the MBR’s send method matches configured send method.</td></tr>
<tr><td>Service Type</td><td>For MBR level tags the configured tag may only be active while there are one or more active services matching Service Type within the MBR. Additionally if Parent Service Category, Service Category, Service Tag or Pay Period is selected they must all match at least one instance of the SAME active service of the MBR.

For Service level tags the configured tag may only be active while the services service type matches.</td></tr>
<tr><td>Service</td><td>For MBR level tags the configured tag may only be active while there are one or more</td></tr>
</table>

Category	active services matching Service Category within the MBR. Additionally if Service Type, Service Tag, Parent Service Category or Pay Period is selected they must all match at least one instance of the SAME active service of the MBR. For Service level tags the configured tag may only be active while the services service category matches.
Service Tag	For MBR level tags the configured tag may only be active while there are one or more active services having a service type configured with Service Tag within the MBR. Additionally if Service Type, Parent Service Category, Service Category or Pay Period is selected they must all match at least one instance of the SAME active service of the MBR. For Service level tags the configured tag may only be active while the service has a service type with a matching service tag.
Pay Period	For MBR level tags the configured tag may only be active while there are one or more active services matching Pay Period within the MBR. Additionally if Service Type, Service Tag, Parent Service Category or Service Category is selected they must all match at least one instance of the SAME active service of the MBR. For Service level tags the configured tag may only be active while the services pay period matches.
Parent Service Category	For MBR level tags the configured tag may only be active while there are one or more active services matching Parent Service Category within the MBR. Additionally if Service Type, Service Category, Service Tag or Pay Period is selected they must all match at least one instance of the SAME active service of the MBR. For Service level tags the configured tag may only be active while the services parent service category matches.
Address Type	Indicates type of address to be used for location specific matching. **Address Type** / **Description** None: Indicates no address matching is needed. When selected address related fields: Country, State, City, Postal Code and Address Data Field are hidden from view within market tag configuration Billing: Use MBR billing address for location matching Shipping: Use MBR shipping address for location matching Service: For service level tags use service address of the service For MBR level tags use the MBR service address default
Country	If configured tag can only be active when accounts address type dependent country field matches configured country.
State	If configured tag can only be active when accounts address type dependent state field matches configured state.
City	If configured tag can only be active when accounts address type dependent city field matches configured city.
Postal Code	If configured tag can only be active when accounts address type dependent postal code field matches configured postal code.
Address Data Field	If configured tag can only be active when accounts address type dependent address data field matches configured address data below.
Address Data	When an address data field is selected this provides matching value for address data field above.
Promo Code	If configured tag can only be active within accounts where an MBR promo code is activated matching configured promo code.
Access Time	If configured tag can only be active while conditions of access time are true excluding time of day. See Common fields for more information on formatting of access time.
Start Date	If configured tag can only be active when the current date is equal or greater than start

<table>
<tr><td></td><td>date.</td></tr>
<tr><td>End Date</td><td>If configured tag can only be active when the current date is less than end date.</td></tr>
<tr><td>Service Created Before</td><td>If configured tag can only be active when the initial service creation date is earlier than "service created before" date. Service creation date represents the time the service was initially added to the MBR regardless of any subsequent use or change.</td></tr>
<tr><td>Service Created After</td><td>If configured tag can only be active when the initial service creation date is later than "service created after" date. Service creation date represents time the service was initially added to the MBR regardless of any subsequent use or change.</td></tr>
<tr><td>Service Counting</td><td>Determines how service count will be determined. If service counting is set to a value other than Disabled service counting fields appear below allowing minimum and maximum service counts to be configured.

<table>
<tr><th>Counting Option</th><th>Description</th></tr>
<tr><td>Disabled</td><td>Service counting will not be performed. Related count fields are hidden from view.</td></tr>
<tr><td>Service - Service Category</td><td>Count number of active services within the services service category sharing a common parent (or root) service.</td></tr>
<tr><td>Service - Service Type</td><td>Count number of active services matching the services service type and sharing a common parent (or root) service.</td></tr>
<tr><td>Service - Any Service</td><td>Count number of active services sharing a common parent (or root) service.</td></tr>
<tr><td>Service - This Service</td><td>Counts only current service. Intended for use in conjunction with service level "service quantity" field.</td></tr>
<tr><td>MBR - Service Category</td><td>Count number of active services sharing services service category within the MBR.</td></tr>
<tr><td>MBR - Service Type</td><td>Count number of active services sharing the services service type within the MBR</td></tr>
<tr><td>MBR - Any Service</td><td>Count number of active services within the MBR</td></tr>
</table></td></tr>
<tr><td>Service Count Min</td><td>If configured tag can only be active when the service is the nth or more in sequence of counted services. For example there are 100 active services in total within an account and a market tag is needed to apply discounting conditionally after the first 20 of 100 services pay full non-discounted rate.

Each of the 100 services sees a different 'service count' based on its relative position within the list of 100 services. The first service of 100 sees 1 (itself) as there is nothing before it and the very last service sees 100 (all 99 preceding services + itself).

In the example scenario above setting service count min to 20 means market tag would apply starting with 20th service in sequence.

When individual services contain a service quantity greater than 1 only result after adding service quantity is evaluated. As an example if service count min is 2, service quantity is 2 and the MBR contains only this service this condition will be considered matched for the service. If service count min is used where it is important for one of the services in this scenario to not match then separate services should be added under the MBR and use of service quantity greater than 1 avoided.</td></tr>
<tr><td>Service Count Max</td><td>Identical to "service count min" above except tag is active when the service is the nth or less in sequence of services within the account. In the above example if service count max is set 20 this means the tag is active for first 20 services and inactive for services 21 thru 100.

When individual services contain a service quantity greater than 1 only result after adding service quantity is evaluated. As an example if service count max is 10, service quantity is 20 and the MBR contains only this service this condition will be considered not</td></tr>
</table>

	matched for the service as 20 exceeds the maximum 10. If service count max is used where it is important for the first 10 services to match and the remaining 10 not match then separate services should be added under the MBR and use of service quantity greater than 1 avoided.
Service Count Total Min	If configured tag can only be active when the total number of counted active services is equal or greater than service count total min. This setting differs from "service count min" in that every counted service sees the same total regardless of its position in the list of active counted services. For example if there are 100 active services in the account and service count total min is set to 20 then the service count total min condition is met for all 100 services rather than only services 20 thru 100 as would be the case with "service count min" option.
Service Count Total Max	Identical to "service count total min" except tag is active when total number of counted active services is equal or less than service count total max.
Invoiced Days Max	If configured tag can only be active while total number of days the service has been invoiced while this tag is active does not exceed "invoiced days max". Every month invoiced while this tag remains active is counted as 30 days regardless of actual number of days within a given month.
Service Months Min	If configured tag can only be active while service has been invoiced for number of months equal to or greater than "service months min". Service months differ from invoiced days in that service month counts are relative to number of months service has been invoiced throughout its history independent of status of this market tag over time.
Service Months Max	If configured tag can only be active when service has been invoiced for number of months equal to or less than "service months max". Service months differ from invoiced days in that service month counts are relative to number of months service has been invoiced throughout its history independent of status of this market tag over time.
Allow Access Time	When set "yes" operators are given the opportunity to configure an access time to control when manual tag will be active while activating tag at MBR or service level. See Common fields for more information on formatting of access time.
Allow Service Cost	When set "yes" a custom static service cost can be associated with the market tag applicable while the tag is active. If there are multiple active market tags which assign a static cost the tag with the highest sort order is used.
Allowed Invoiced Days Max	When set "yes" a custom "invoiced days max" can be applied to the market tag when manually activating the tag from service level market tags menu.
Copy Service Cost	When set "yes" service cost field below is automatically copied to service cost field when manually activating a market tag from services market tag menu. Since service level tag static cost overrides the configured service cost below this enables per service pricing to not be affected by subsequent changes to the service cost field below. When set "no" cost is not automatically copied and if operator decides not to set a service cost within the service then any service cost configured below at the market tag level is used. This allows for changes to market tag to affect existing account pricing.
Service Cost	When set normal service pricing is overridden for any service where this tag is activate. Service cost always represents the monthly cost of service regardless of the pay period of the account. If multiple market tags set service cost the tag with the highest sort order is used to determine service cost.
Service Discount	If a discount is set any service where this tag is active will received the associated discount. If there are multiple active tags with multiple discounts each applicable discount type is applied to the remaining amount after previous discounts during

<table>
<tr><td></td><td>invoicing. Order multiple discounts are applied is determined by sort order field starting with lowest sort order in ascending order.</td></tr>
<tr><td>ETF Type</td><td>Offers option to automatically assess an early termination fee should service be canceled permanently before the ETF term has completed.

<table>
<tr><th>ETF Type</th><th>Description</th></tr>
<tr><td>None</td><td>No ETF charges will be assessed and remaining ETF related fields are hidden from view.</td></tr>
<tr><td>Fixed amount</td><td>If service is closed permanently prior to completion of ETF term then amount of the ETF charge is the full amount of the ETF charge type regardless of remaining contract term.</td></tr>
<tr><td>Ratio of time remaining to fixed fee</td><td>If service is closed permanently prior to completion of ETF term then amount of the ETF charge is the percentage of the ETF charge type representing the remaining contract term.

For example if ETF term is 36 months, account is canceled after 24 months and ETF charge type is $30 then the ETF amount is $10 for the remaining year out of the three year term.</td></tr>
<tr><td>Amount times remaining months</td><td>If service is closed permanently prior to completion of ETF term then amount of the ETF charge is the ETF charge type amount multiplied by the number of remaining months of the service term.

For example if ETF term is 36 months, account is canceled after 24 months leaving 12 month remaining term and the ETF charge type is $10 the total calculated ETF fee is $120 ($10 for each of remaining month).</td></tr>
</table></td></tr>
<tr><td>ETF Charge Type</td><td>Charge type to be used for ETF line item when an ETF fee is assessed. Cost assigned to the charge type affects ETF fee based on selected ETF Type above.</td></tr>
<tr><td>ETF Term (Months)</td><td>Months tag must be active for ETF charges to not apply if service is closed with a permanent cancel reason. ETF term does not represent total number of months the service has been previously invoiced or number of months since initial activation as tag may become inactivate and no longer count during inactive period. For example if service has been temporarily closed or tag matching condition fails.</td></tr>
<tr><td>ETF Min Service Level</td><td>Prevents customer from downgrading service to a service lower than the configured service level prior to conclusion of the ETF Term. Service levels are configured as part of association of service types to service categories from Emerald Admin / Services / Service Categories.</td></tr>
<tr><td>Active</td><td>When inactive the tag is not available to be selected as a manual tag from MBR and Service menus. Tag is also inactivated globally within any MBRs or Services currently using the tag. Inactivating a market tag does not retroactively affect invoicing terms where account has already been invoiced for service with the tag active.</td></tr>
<tr><td>Sort Order</td><td>Determines order in which static costs and discounts directly associated with active market tag are applied with lowest sort orders applied first. For static cost the matching market tag with the lowest sort order is selected. With discounting all matching discounts are applied in order of lowest to highest sort. If multiple matching tags have the same sort order tags created earlier come before tags created later. See also Common fields</td></tr>
</table>

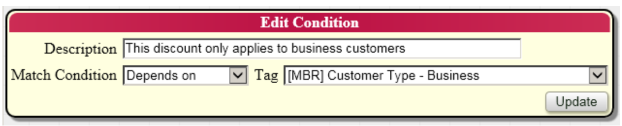
Condition Matching

In addition to matching conditions configured above automatic tags may be configured to require other MBR or Service level tags in either an active or inactive state.

Examples include "promotional discounts are incompatible with pay period discounts" or "business loyalty discount requires both business tag and 1 year of service tag".

Tags can depend on or conflict with each other in any order or arrangements however care should be taken to logically organize tags and minimize dependencies to reduce management effort. A layered approach is recommended consisting generally of the following.

1. Tags representing basic facts
2. Composite tags matching combinations of basic facts
3. Additional groupings of composite tags
4. Tags matching previous layers to apply changes such as assigning discounts, ETF and RADIUS authorization.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Optional informational label describing reason for condition</td></tr>
<tr><td>Match Condition</td><td>Determines whether match condition shall require referenced tags to be in an active or inactive state.

<table>
<tr><th>Match Condition</th><th>Description</th></tr>
<tr><td>Depends on</td><td>Tag can only be active when the referenced tag is also active.</td></tr>
<tr><td>Conflicts with</td><td>This condition roughly means tag can only be active when the referenced tag is not active.

More specifically it indicates either tag or referenced tag may be active but not both preferring a solution in which tag will not be active while referenced tag is also active.

This preference to inactivate tag rather than referenced tag is typical but not absolute. It is unlikely but possible for referenced tag to become inactive as a result of tag being active. The only guaranteed outcome is both tag and referenced tag will never be concurrently evaluated as active.

Overuse of 'conflict' match condition can lead to solutions having many equally valid answers for which solution expected by operators may differ from outcome selected by market engine.</td></tr>
<tr><td>Depends on all</td><td>Tag can only be active when all tags comprising the referenced tag group are also active. If any tag within the referenced group is inactive the tag will not be active.</td></tr>
<tr><td>Depends on any</td><td>Tag can only be active when at least one tag within the referenced group is also active. If all tags within the</td></tr>
</table>
</td></tr>
</table>

		referenced group are inactive then tag will not be active.
	Conflicts with any	This condition roughly means tag can only be active when all tags within the referenced tag group are not active. If one or more tags within the referenced group are active then tag will not be active. More specifically it indicates either tag or every referenced tag within the tag group may be active but not both preferring a solution in which tag will not be active while any tags in the referenced tag are active. This preference to inactivate tag rather than referenced tag group is typical but not absolute. It is unlikely but possible for all members of referenced tag group to become inactive as a result of tag being active. The only guaranteed outcome is both tag and all members of referenced tag group will never be concurrently evaluated as active. Overuse of 'conflict with any' match condition can lead to solutions having many equally valid answers for which solution expected by operators may differ from outcome selected by market engine.
Tag	When using 'depends on' or 'conflicts with' match condition tag represents the referenced tag.	
Tag Group	When using 'depends on all', 'depends on any' or 'conflicts with any' match conditions tag group represents the referenced tag group.	

Process Actives

Within market tags menu the "Process Actives" option when selected recalculates current day's active markets across all active MBRs and services within the system. Reprocessing of tag status is normally handled automatically via scheduled task at the start of each day however if changes are made to market tags that may globally affect tag status process actives provides a means of reprocessing all tags right away.

It is important to note active status is mostly informational in nature to provide operators with list of active tags when viewing MBRs and services. Depending on configuration active tags may also influence RADIUS authorization.

Active status has no effect on invoicing activities. It is not necessary to process actives to ensure accurate invoicing with respect to calculation of market tags.

Market Categories

Market tags are organized into market categories which provide for grouping of related tags. Each market tag is required to be assigned to exactly

New Category

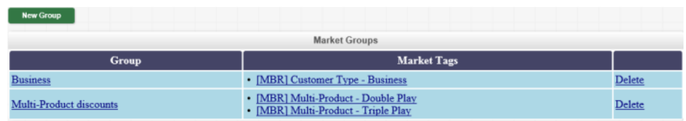
Market Categories

Market Category	Market Tags	Sort Order	
Customer Type	• [MBR] - Business • [MBR] - Household • [Service] - Service Business • [MBR] - Wireless	0	Delete
ETF	• [Service] - Campsite ETF	0	Delete
Uncategorized	• [Service] - Wireless turbo boost • [Service] - Static Cost	0	Delete
Multi-Product	• [MBR] - Double Play • [MBR] - Triple Play • [Service] - Triple Play - IPTV Discount • [Service] - Triple Play - Voip Discount • [Service] - Triple Play - Wireless Discount	100	Delete
Mutli-Product Base	• [MBR] - Hosting • [MBR] - IPTV Services • [MBR] - Voice Services • [MBR] - Wireless	100	Delete

one market category. Market categories are exclusively informational.

Field	Description
Description	Unique label describing market category
String ID	See Common fields
Sort Order	See Common fields

Market Groups



Like "market categories" "market groups" also provide for grouping of related market tags with the following differences.

- Market groups are not required
- A market tag can belong to any number of market groups
- Groups are used primarily for applying group based condition matching when using condition types "Depends on all", "Depends on any" and "Conflicts with any".

An example use of market group would be creating a group labeled "Pay Period Discounts" associating all market tags offering discounting based on pay period with the "Pay Period Discounts" group. This group could then for example be referenced using "Conflicts with any" condition by market tags which offer multi-product or loyalty discounts to prevent both pay period and multi-product discounts from applying at the same time to a service. Without grouping a conflict condition would have to have been applied against each pay period discount tag to achieve the same result. Groups offer advantages in reduced configuration and improved organization of market tag dependencies.

INVENTORY

Inventory offers configuration and tracking of physical goods for sale or assigned to facilitate network access. Also supported are provisioning virtual items such as IP address, IP subnet and telephony DID.

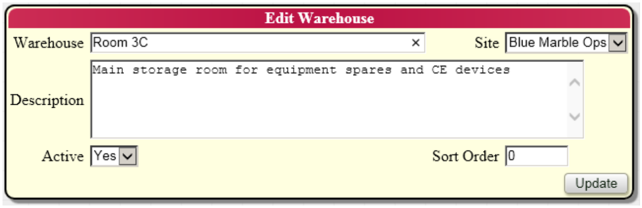
Warehouses

Warehouses define distinct fixed or mobile locations where physical items are available to be stocked. Once defined one or more warehouses may be assigned to each product to determine where product may be stored as well as target stocking levels.

New Warehouse

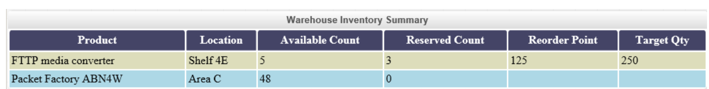
Warehouses

Warehouse	Site	Description	
Building 1A	Installer Depot	First building on the right	Delete
Building 2B	Installer Depot	Across the street from building 1	Delete
Little storage box of holding	Blue Marble Ops	This warehouse is surprisingly spacious	Delete
Room 3C	Blue Marble Ops	Main storage room for equipment spares and CE devices	Delete
Truck 1	Installer Depot	License #BLUNET1	Delete



Field	Description
Warehouse	Unique name of warehouse, storage area or vehicle where items are to be stocked
Site	Physical location of warehouse
Description	Additional details about this warehouse
Active	When "Yes" warehouse is available to for new inventory items to be assigned and the warehouse is included in stocking reports. When "No" new inventory items may not be transferred however items having been already assigned remain unaffected.
Sort Order	See Common fields

When one or more products have been assigned to a warehouse an inventory summary is displayed below edit warehouse form providing information about each product including current stocking level of all items currently assigned to this warehouse.

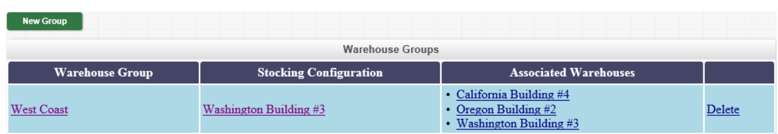


Warehouse Inventory Summary

Product	Location	Available Count	Reserved Count	Reorder Point	Target Qty
FTTP media converter	Shelf 4E	5	3	125	250
Packet Factory ABN4W	Area C	48	0		

Warehouse Groups

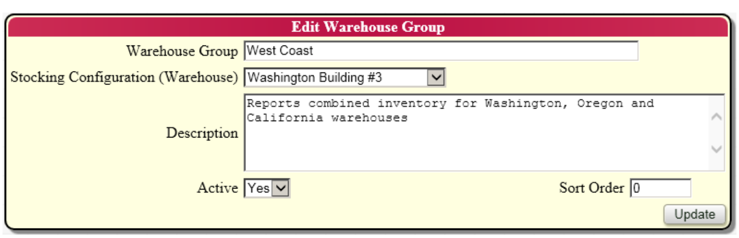
Related warehouses can be organized together using to assist with inventory reporting from this menu. For example in addition to running reorder report at individual warehouse level groups enable reporting at regional or global levels across two or more warehouses.



New Group

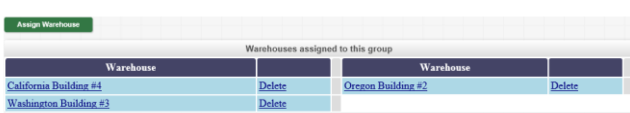
Warehouse Groups

Warehouse Group	Stocking Configuration	Associated Warehouses	
West Coast	Washington Building #3	• California Building #4 • Oregon Building #2 • Washington Building #3	Delete



Field	Description
Warehouse Group	Label uniquely describing role of this group
Stocking Configuration	Selects warehouse containing product stocking settings to be used for reorder and

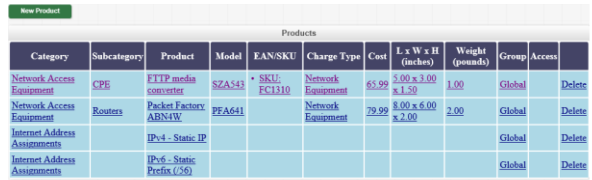
	related stock level reporting. Warehouse selected for this purpose need not match a warehouse assigned to the warehouse group. This setting only selects product stocking configuration to be used by the group. It does not include the warehouse as a member of the group. A couple of common scenarios are described below. First a series of regional warehouse groups all using a common "Warehouse Regional" for stocking data: • Region A ○ Warehouse A1 ○ Warehouse A2 ○ Warehouse A3 • Region B ○ Warehouse B1 ○ Warehouse B2 • Region C ○ Warehouse C1 ○ Warehouse C2 A warehouse group is created for each of the three regions and corresponding warehouses within that region are assigned to the warehouse group. However in this case the stocking configuration warehouse for all three warehouse groups is "Warehouse Regional" which offers generic stocking levels similar across all three regional groups. "Warehouse Regional" warehouse is not assigned to any of the three regional warehouse groups. In the second example a master warehouse has a few small satellite warehouses including inventory stored in vehicles. • Master Warehouse ○ Storage building A ○ Installer vehicle B ○ Installer vehicle C To configure a warehouse group that will report on all inventories across master warehouse and its satellites "Master Warehouse" is set as stocking configuration AND also assigned to the warehouse group such that the warehouse group is associated with "Master Warehouse", "Storage building A", "Installer vehicle B" and "Installer vehicle C"
Description	Additional information and notes specific to this group
Active	When inactive the group is hidden from view and not included with any reporting data
Sort Order	See [Common fields]

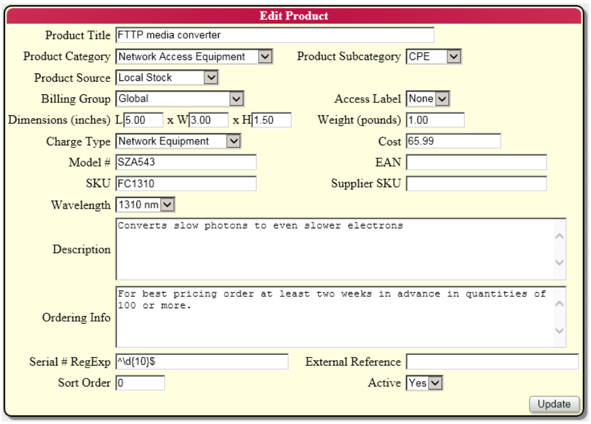


Once a new group is created options appear immediately below the edit form to associate any number of warehouses with the group.

Products

Details of each product available for sale or assigned to customer are configured within products menu. Once a product has been added associated inventory is able to be stocked from "Receive Items" menu of Emerald Client Inventory menu. Prior to configuring products it is recommended supporting configuration including Product Categories, Product Sources, Charge Types and Product Attributes be setup.



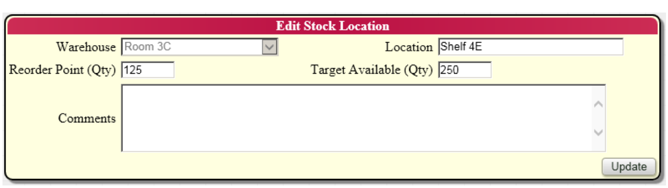


Field	Description
Product Title	Unique label of product appearing when selecting inventory for purchase or assignment to services. Title should include all relevant information to enable operators to uniquely identify and select this product.
Product Category	Selection of product category this product is to be grouped with. Membership may include category specific product and item level custom data attributes. Product category is required.
Product Subcategory	Subcategory within product category to further group this product. Subcategory is optional.
Product Source	Determines where and how this product is sourced. Sources can affect products in a number of ways: Customization of receiving interface, inventory reporting, ability to assign inventory to services and any RADIUS attributes associated with assigned items. See source types in Product Sources for more information.
Auto Unassign State	When not disabled and an item of this product is assigned to a service that is subsequently inactivated or permanently canceled the item in inventory will be automatically unassigned from the service and set to the selected state. There may be up to a three day delay between inactivation or permanent cancel and automatic unassignment of service assigned inventory item.
Billing Group	See Common fields
Access Label	See Common fields
Dimensions (LxWxH)	Length, Width and Height of the product including all product packaging in operator configured units.
Weight	Total weight of product in operator configured units.
Charge Type	If product is sold via POS invoice charge type is used to define the charge type of the invoice line item for reporting and tax purposes.
Supplier Cost	Default price charged by supplier to obtain product. This field is only used for informational reporting purposes and does not control price charged to customers as inventory is sold. Item level supplier cost takes precedence over product level supplier cost.

Customer Cost	Default product level cost to be charged if inventory item of product is sold via POS invoice. Item level customer cost takes precedence over product level customer cost.
Model #	Vendor supplied model number
EAN	Vendor supplied EAN
SKU	Vendor or internal SKU
Supplier SKU	Supplier SKU for reordering. This field is displayed in the reorder report.
*** Custom data	Additional custom product level fields are displayed based on attributes assigned at the product category, subcategory and product levels. Fields can be either selection lists or input fields with optional regular expression based format validation
Description	Additional detail about product and capabilities. This information is informational to assist operators to select the correct package.
Ordering Info	Information related to reordering this product. This field is displayed in the reorder report.
Serial # RegExp	A Perl compatible regular expression for restricting data entry format to valid serial numbers for this product. This is used for input validation as well as automatic advancement when recording inventory using barcode scanner. The design and troubleshooting of regular expressions is not supported.
External Reference	See Common fields
Sort Order	See Common fields
Active	When "Yes" product is available for receiving new inventory. When "No" inventory may not be received for this product and product appears as inactive within selection lists. Product is excluded from reorder and stocking reports. Active status of product does not affect existing items of this product previously assigned to services.

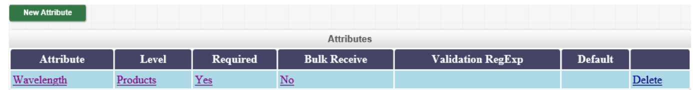
Product Stocking Locations

Once a product is created one or more warehouses can be assigned to indicate where product inventory is located. This data is used during warehouse selection when receiving inventory as well as inventory reporting.

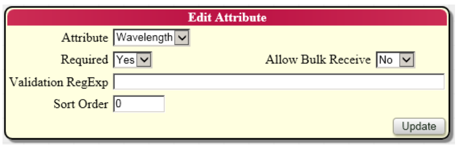


Field	Description
Warehouse	Location where this product may be stored. See Warehouses.
Location	Specifies an area such as a room, shelf or rack where this particular product can be located within selected warehouse.
Reorder Point (Qty)	Level of available inventory of this product at warehouse below which more should be ordered. Field is used in reorder reporting to determine when to recommend reordering more of this product.
Target Available (Qty)	A target stocking level for this product at selected warehouse.
Comments	Additional information about warehouse, location or product.

Attributes

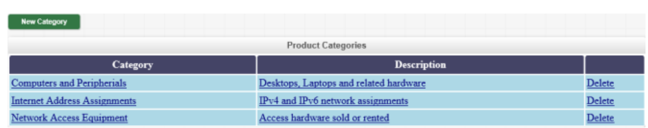


Attributes enable additional data fields specific to the product to be included with product configuration when managing product or to inventory items when new inventory is received or changed. In order for attributes to be assignable to a product they are first defined within Product Attributes menu.

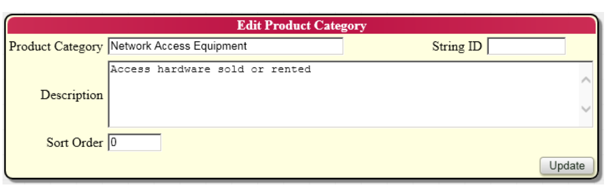


Field	Description
Attribute	Selection of custom data field to be assigned to this product or inventory item. See Product Attributes.
Required	When "Yes" a value for this field is expected to be entered at the product or inventory item level. When "No" the field may be ignored and no value entered.
Allow Bulk Receive	If the selected attribute applies to inventory items and this is set "Yes" the attribute appears as a data field when receiving inventory.
Default Value	When an item level attribute is selected a default value can be chosen when receiving new items. Default values are applied only to item level data at the time new items are recorded into inventory. Changing a default value has no effect on pre-existing items record to inventory prior to change. This setting is unavailable for product level attributes.
Validation RegExp	A Perl compatible regular expression for restricting data entry format for input validation. The design and troubleshooting of regular expressions is not supported.
Sort Order	See Common fields

Product Categories



Product categories enable similar types of products to be grouped together and optionally further organized into subcategories. This organization makes products easier to locate and enables assignment of category specific data fields at product and inventory item levels.



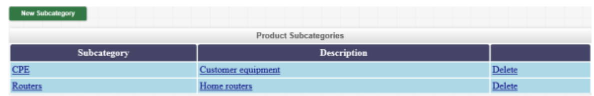
Field	Description
Product Category	Label uniquely describing the product category
String ID	See Common fields
Description	Additional details related to product category
Sort Order	See Common fields

Attributes

Enables assignment of product and item level data fields to any product associated with this product category. For configuration details see Attributes.

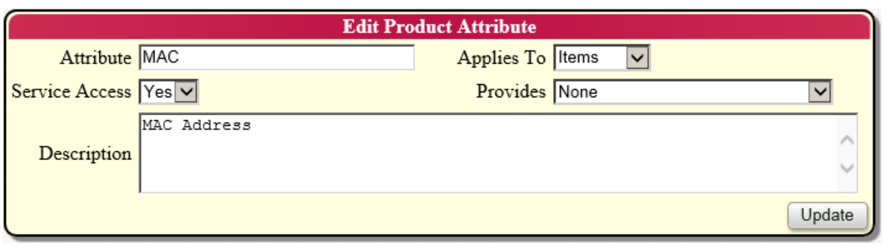
Product Subcategories

An optional secondary grouping of products within a product category is enabled by adding one or more Subcategories. Configuration of subcategory is identical to product category.



Product Attributes

Attributes are custom data fields assignable at product category, subcategory and product levels to products as well as individual inventory items. Attributes without any values assigned to it are displayed as input fields. When one or more value is assigned to an attribute the field appears as a selection box.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Attribute</td><td>Label of the data field to appear when adding or changing a product or inventory item</td></tr>
<tr><td>Applies To</td><td>Determines whether data field will be available at the product level or separately for each inventory item of the product.</td></tr>
<tr><td>Service Access</td><td>When 'Yes' item level attribute values can be changed from service level inventory menu.
When 'No' item level attribute values can only be changed from main inventory menu.</td></tr>
<tr><td>Provides</td><td>Maps custom attributes to internal data fields used for reasons described in the table below.

Normally 'None' is selected to disable mapping. When attributes are mapped the mapped attributes data validation rules are enforced ignoring any custom validation expressions that may have been configured.

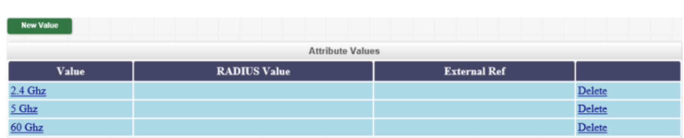
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>None</td><td>No mapping is performed</td></tr>
<tr><td>Service Transmit Power (dBm)</td><td>Required for calculation of tower link margin.

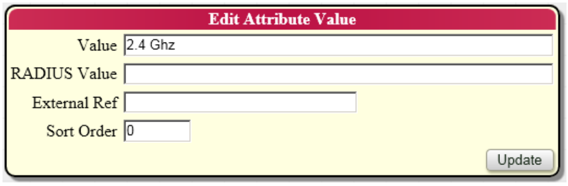
Only one attribute of this type should be defined for inventory assigned to any single service. If there are multiple instances the</td></tr>
</table>
</td></tr>
</table>

		value having lowest transmit power is used. If specified at both item and product level item level data is used instead of product level data.
	Service Receive Sensitivity (dBm)	Required for calculation of service link margin. Only one attribute of this type is recommended to be defined for inventory assigned to any single service. If there are multiple instances the value having lowest sensitivity is used. If specified at both item and product level item level data is used instead of product level data.
	Service Antenna Gain (dBi)	Required for calculation of service and tower link margins. Only one attribute of this type should be defined for inventory assigned to any single service. If there are multiple instances the value having lowest transmit power is used. If specified at both item and product level item level data is used instead of product level data.
	Service Additional Gain (dB)	Optional sources of additional gain (e.g. add-on antenna elements, amplifiers) influencing both service and tower link margins. If there are multiple instances of this attribute in assigned inventory all instances are summed together. If specified at both item and product level item level data is used instead of product level data.
	Service Additional Loss (dB)	Optional sources of added loss (e.g. cables and connectors) influencing both service and tower link margins. Loss must be entered as a negative value. If there are multiple instances of this attribute in assigned inventory all instances are summed together. If specified at both item and product level item level attribute takes precedence over any product level data.
Show In Search Results	When 'Yes' table of inventory search results include this attribute as a separate column when one or more items included with search result have a value for this attribute. This setting is applicable only to item level attributes.	
Description	Additional information detailing use of the data field	

Attribute Values

If data field is to allow text or numeric input then no attribute values should be assigned to the attribute. If one or more attributes are added then the data field is presented as a selection list.



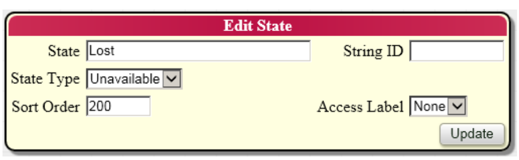


Field	Description
Value	Value to be displayed within the data fields selection list
RADIUS Value	If a products product source defines RADIUS attributes which reference this attribute then value entered here is transmitted with RADIUS authorization attributes. If RADIUS Value is not specified then Value is transmitted in its place.
External Ref	See Common fields
Sort Order	See Common fields

Product States

Product states offer ability to define disposition of every inventory item tracked by Emerald. Typical examples of states include: available, lost, sold, assigned and damaged. Selection list of states for a given product is determined by product source selected within the products configuration.

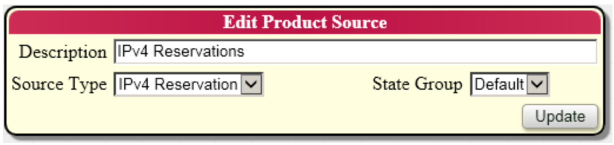
Once a state group has been created states can then be associated with the group. It is required for each state group for at least one state covering state types Available, Allocated and Unavailable to have been configured.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>State</td><td>Label describing disposition of inventory item. State appears as selection option when managing inventory items and also reflected in inventory reporting.</td></tr>
<tr><td>String ID</td><td>See Common fields</td></tr>
<tr><td>State Type</td><td>State types determine how this state is to be treated by Emerald for the purposes of inventory management.
<table><tr><th>State Type</th><th>Description</th></tr><tr><td>Available</td><td>Item is available for purchase or assignment to service</td></tr><tr><td>Reserved</td><td>Item is stocked but is reserved for a reason classified by reserve type</td></tr><tr><td>Allocated</td><td>Item has been assigned to a service for use</td></tr><tr><td>Unavailable</td><td>Item is no longer available</td></tr></table></td></tr>
<tr><td>Reserve Type</td><td>When state type is reserved then reserve type field is displayed to input additional information related to the reservation. This field is reserved for future use and custom workflows.</td></tr>
<tr><td>Sort Order</td><td>See Common fields</td></tr>
<tr><td>Access Label</td><td>See Common fields</td></tr>
</table>

Product Sources

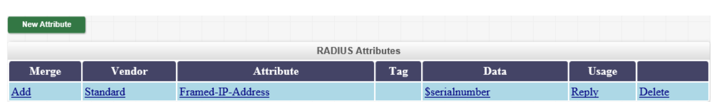
Product sources defines where products are obtained as well as influence RADIUS authorization to support assignment of addressing resources (IPv4, IPv6 and DID) from inventory and authorization of inventory specific identifiers (MAC address or serial number).

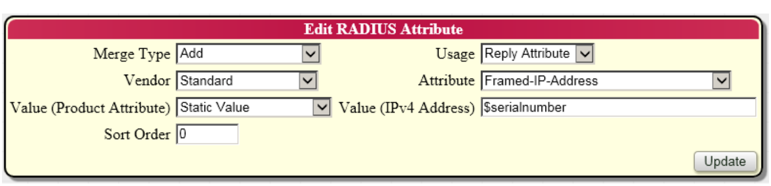


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Unique label of source such as name of specific vendor or distributor</td></tr>
<tr><td>Source Type</td><td>While largely informational source types can affect process of receiving new inventory.
<table>
<tr><th>Source Type</th><th>Description</th></tr>
<tr><td>Stocked Item</td><td>Indicates items from this source are intended to be used primarily for sale to customers.</td></tr>
<tr><td>Stocked Rental</td><td>Indicates items from this source are intended to be used primarily for assignment to services. Products assigned to this source type are available for assigning product requirements to service types.</td></tr>
<tr><td>Drop Ship</td><td>Indicates items is ordered as needed on behalf of end users and not stocked locally. This option is reserved for future use.</td></tr>
<tr><td>IPv4 Reservation</td><td>Indicates items will be IPv4 addresses or subnets and provides IPv4 specific tools for management of address resources. Products assigned to this source type are available for assigning product requirements to service types.</td></tr>
<tr><td>IPv6 Reservation</td><td>Indicates items will be IPv6 prefixes and provides IPv6 specific tools for management of prefixes. Products assigned to this source type are available for assigning product requirements to service types.</td></tr>
</table></td></tr>
<tr><td>State Group</td><td>Represents group of product states available to manage disposition of products assigned to this product source.</td></tr>
</table>

RADIUS Attributes

To support allocation of network identifiers from inventory RADIUS authorization response can be modified when inventory items are assigned to services where assigned product has a matching product source.

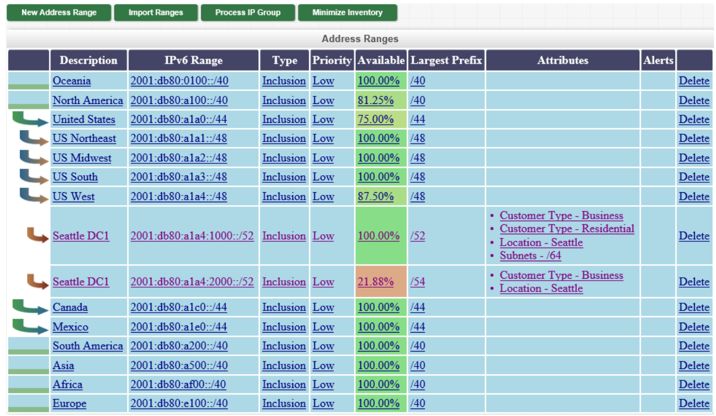




<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Merge Type</td><td>Configures how any RADIUS attributes are to be integrated with existing RADIUS reply or check attributes of an authenticating session.
<table>
<tr><th>Merge Type</th><th>Description</th></tr>
<tr><td>Add</td><td>Attribute will be unconditionally appended to RADIUS authorization response.</td></tr>
<tr><td>Add or replace value</td><td>Attribute will be added if an existing RADIUS authorization response attribute of the same vendor and attribute does not exist. If a matching attribute already exists then its value will be updated.</td></tr>
<tr><td>Delete</td><td>If the selected vendor and attribute exists in the current RADIUS authorization response it will be unconditionally removed from response.</td></tr>
<tr><td>Delete matching</td><td>If the selected vendor and attribute exists in the current RADIUS authorization response it will be conditionally removed from response when its value matches configured value.</td></tr>
<tr><td>Replace value</td><td>If an existing RADIUS authorization response contains a matching vendor and attribute then the value of that attribute will be replaced with configured value. If there is no vendor + attribute match then no changes are made.</td></tr>
</table></td></tr>
<tr><td>Usage</td><td>Determines whether attributes will be applied to RADIUS authorization response as reply attributes or confirm authentication parameters as check attributes.
<table>
<tr><th>Usage</th><th>Description</th></tr>
<tr><td>Reply attribute</td><td>Indicates that RADIUS attribute is to be included in authorization response transmitted in Access-Accept. This is the default and most commonly used usage setting.</td></tr>
<tr><td>Check attribute</td><td>Indicates RADIUS attribute is to be checked against incoming authentication attributes transmitted in Access-Request to make sure the values of attributes agree. If there is no match then authentication fails.</td></tr>
</table></td></tr>
<tr><td>Vendor</td><td>Vendor associated with selected attribute</td></tr>
<tr><td>Attribute</td><td>Vendor dependent RADIUS attribute</td></tr>
<tr><td>Value (Product Attribute)</td><td>When "Static Value" a secondary value field is offered to accept manual configuration of value. When any other value the RADIUS value of the product attribute at item or product level is used as the RADIUS attributes value.</td></tr>
<tr><td>Value</td><td>When product attribute value field above is "Static Value" the static value desired for chosen attribute is entered into this field.</td></tr>
<tr><td>Applies To</td><td>Determines which service this attribute is assigned. Typical recommended setting is "Self".
<table>
<tr><th>Applies To</th><th>Description</th></tr>
<tr><td>Self</td><td>Attribute will be applied directly to the service account</td></tr>
<tr><td>Parent Service</td><td>Attribute will be applied to the services parent service</td></tr>
</table></td></tr>
<tr><td>Sort Order</td><td>Determines order attributes within the group of attributes assigned from inventory are to be merged and appear in RADIUS authorization Access-Accept response.</td></tr>
</table>

IP Groups

IP groups act as an integrated IP address management (IPAM) facility to view, organize and assign available addressing resources. IPv6, IPv4 and 64-bit integer sequences for telephony and custom applications are supported.



New Address Range | Import Ranges | Process IP Group | Minimize Inventory

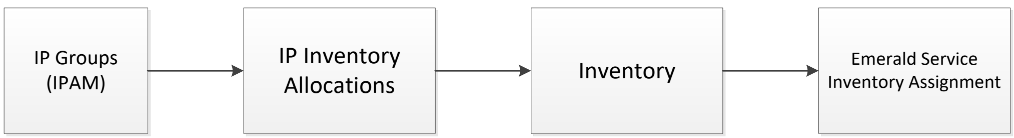
Address Ranges

	Description	IPv6 Range	Type	Priority	Available	Largest Prefix	Attributes	Alerts	
	Oceania	2001:db80:0100::/40	Inclusion	Low	100.00%	/40			Delete
	North America	2001:db80:a100::/40	Inclusion	Low	81.25%	/40			Delete
	United States	2001:db80:a1a0::/44	Inclusion	Low	75.00%	/44			Delete
	US Northeast	2001:db80:a1a1::/48	Inclusion	Low	100.00%	/48			Delete
	US Midwest	2001:db80:a1a2::/48	Inclusion	Low	100.00%	/48			Delete
	US South	2001:db80:a1a3::/48	Inclusion	Low	100.00%	/48			Delete
	US West	2001:db80:a1a4::/48	Inclusion	Low	87.50%	/48			Delete
	Seattle DC1	2001:db80:a1a4:1000::/52	Inclusion	Low	100.00%	/52	• Customer Type - Business • Customer Type - Residential • Location - Seattle • Subnets - /64		Delete
	Seattle DC1	2001:db80:a1a4:2000::/52	Inclusion	Low	21.88%	/54	• Customer Type - Business • Location - Seattle		Delete
	Canada	2001:db80:a1c0::/44	Inclusion	Low	100.00%	/44			Delete
	Mexico	2001:db80:a1e0::/44	Inclusion	Low	100.00%	/44			Delete
	South America	2001:db80:a200::/40	Inclusion	Low	100.00%	/40			Delete
	Asia	2001:db80:a500::/40	Inclusion	Low	100.00%	/40			Delete
	Africa	2001:db80:af00::/40	Inclusion	Low	100.00%	/40			Delete
	Europe	2001:db80:e100::/40	Inclusion	Low	100.00%	/40			Delete

IP groups are comprised of one or more address ranges. As ranges are added or modified they are automatically organized into hierarchies and evaluated for consistency across the IP address group as well as validating subnet/address assignments previously allocated from the group.

Each IP group is separate and independent. No sharing or communication occurs between IP groups. Each group may contain and manage the same address ranges as one or more other groups.

Ranges may be tagged with attributes documenting properties and intended purpose as well as facilitating automatic assignment of address resources.



IP groups working in conjunction with Emerald inventory system is able to continuously maintain desired stocking levels of available addresses. Working together addresses are automatically stocked for assignment to customers and summary of range utilization provides operators with needed details for future planning.

Field	Description
IP Group	Unique label describing intended purpose of the IP group
Address Family	Determines address type of all addresses and address ranges managed by the IP Group. To manage addresses across multiple address families such as both IPv4 and IPv6 a separate IP Group is necessary for each address family.
Active	When 'Yes' configuration changes to the IP Group continue to be evaluated and inventory is allocated from the IP group as needed. When 'No' configuration changes are no longer evaluated and no allocation to inventory occurs.
Sort Order	See Common fields

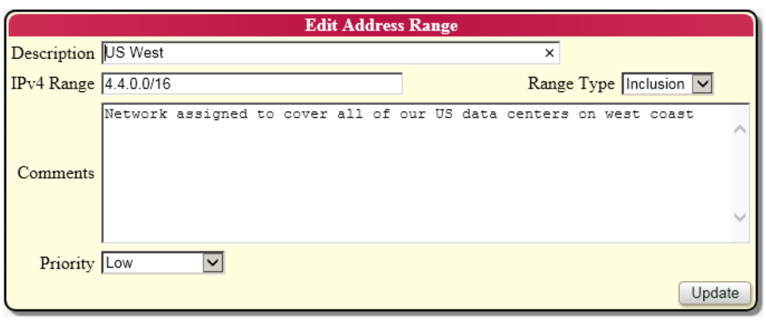
Submenu options available after IP Group creation:

Option	Description
New Address Range	See Address Ranges below.

Import Ranges	Offers bulk CSV flat file import of address ranges into the IP Group. Follow on screen instructions for additional information.
Process IP Group	Fully evaluates the IP Group. If there are no group level alerts raised processing also allocates addresses to inventory as requested by IP Inventory Allocations.
Minimize Inventory	In the event more items are available in inventory than target quantity configured within IP Inventory Allocation clicking this option removes excess available inventory freeing up resources within the IP Group for future assignments. Minimize inventory is only able to remove unassigned addresses currently marked as available for assignment from inventory. This feature does not remove inventory currently assigned to a service or otherwise marked as unavailable. Normally minimize only occurs during processing when there is insufficient free address resources available to meet quantity targets of one or more IP Inventory Allocations. When used in conjunction with adjusting target quantity of corresponding IP inventory allocation this option can be used to remove all previously allocated items from inventory by setting Target Qty 0 in order to change configuration or recover from configuration mistake. This setting has no effect on inventory already assigned to a service or in an unavailable state.

Address Ranges

Address ranges act as "containers" from which addresses and other containers are sourced. Adding ranges that are subsets of existing ranges allows larger ranges to be split up and managed separately for purposes of address allocation and consumption reporting.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Unique label describing address range. Displayed within the IP Groups range listing</td></tr>
<tr><td>*** Range</td><td>Ranges may be entered in the following formats depending on address family of the IP group. Only numbered resources are accepted. DNS names cannot be used.
<table>
<tr><th>Address Family</th><th>Description</th></tr>
<tr><td>IPv4</td><td>Following IPv4 range formats are supported:

10.0.0.1
10.9.8.0/24
10.0.0.100 - 10.0.0.200
10.2.3.*
10.*.*.*</td></tr>
<tr><td>IPv6</td><td>Smallest allowed IPv6 prefix length able to be managed within an IP</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td></td><td>Group is /64. Following IPv6 range formats are supported:

2001:db80::1ea
2001:db80::/32
2001:db80::1000 - 2001:db80::1100</td></tr>
<tr><td>Integer</td><td>Following integer (64-bit unsigned) range formats are supported:

2065551212
2065551000 - 2065551999</td></tr>
</table></td></tr>
<tr><td>Range Type</td><td>Determines whether range shall be available for allocation.

<table>
<tr><th>Range Type</th><th>Description</th></tr>
<tr><td>Inclusion</td><td>Range is eligible to be allocated from. See IP Inventory Allocation.</td></tr>
<tr><td>Exclusion</td><td>Indicates range is already in use elsewhere and will not become available for subsequent allocation from Emerald for any reason.</td></tr>
</table></td></tr>
<tr><td>Comments</td><td>Additional informational</td></tr>
<tr><td>Priority</td><td>Controls order of ranges addresses are assigned from range relative to other applicable ranges within the IP Group. Addresses are first assigned from higher priority ranges before allocation from lower priority ranges is considered.</td></tr>
</table>

RANGE ATTRIBUTES

Once a range is created attributes may be optionally assigned to documenting properties and intended purpose as well as facilitating automatic assignment of address resources. Listings of available attributes are managed from the IP Attributes menu.

IP Inventory Allocations

Allocations of addresses from an IP Group to inventory for eventual service assignment are managed from this menu. Once fully configured allocation occurs whenever the corresponding IP Group is processed by one of the following:

New Allocation

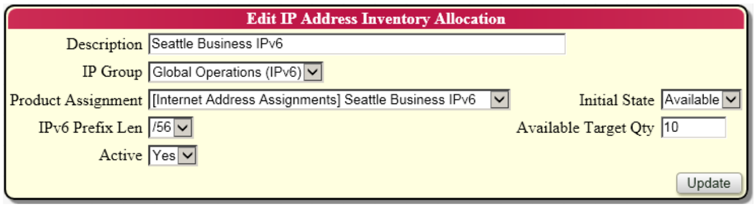
IP Address Inventory Allocations

Description	IP Group	Product	Default State	Prefix Length	Target Qty	Unallocated	Alerts	
Seattle Residential IPv4	Global Operations (IPv4)	IPv4 - Static IP	Available	/32	100	60315		Delete
Seattle Business IPv6	Global Operations (IPv6)	IPv6 - Static Prefix (/60)	Available	/60	200	0		Delete
Seattle Basic Residential voice	Seattle DIDs	Seattle Basic Residential Voice	Available		100	902		Delete
Seattle Premium Business Voice	Seattle DIDs	Seattle Premium Business Voice	Available		200	802		Delete

- Manually clicking 'Process' from corresponding IP Group.
- By default the scheduled task "Process address group inventory allocation" runs periodically at 10 minute intervals. This scheduled task is typically primary means by which addresses are allocated from IP Group to inventory on an ongoing basis to meet demand.

Requirements applied to an allocation allow for resources to be assigned from a subset of appropriate ranges within IP Group either by directly identifying allowed ranges or by attribute matching. When allocating multiple subnets of varying prefix lengths it is recommended dedicated ranges within the IP Group be designated for each prefix length in order to avoid fragmentation maximizing available address resources.

The "Unallocated" column in the allocations listing represents estimated number of remaining addresses of given prefix length available for allocation from IP Group to inventory based on all applicable requirements. Unallocated does not include count of currently available inventory that has been previously allocated or the impacts from competing allocations that may draw from the same ranges.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Unique label describing the allocation</td></tr>
<tr><td>IP Group</td><td>Address group from which to allocate addresses</td></tr>
<tr><td>Product Assignment</td><td>When addresses are assigned to inventory the inventory item created will be of the chosen inventory product. Only one inventory allocation can be assigned to a specific product per IP Group.

Inventory products must be sourced as follows in order for product to be available for selection.

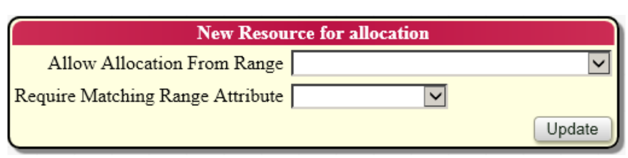
<table><tr><th>IP Group - Address Family</th><th>Inventory - Source Type</th></tr><tr><td>IPv4</td><td>IPv4 Reservation</td></tr><tr><td>IPv6</td><td>IPv6 Reservation</td></tr><tr><td>Integer</td><td>Integer Reservation</td></tr></table></td></tr>
<tr><td>Initial State</td><td>When new inventory items are created they will initially be assigned the selected product state. Only states with a state type of "available" are listed for selection.</td></tr>
<tr><td>*** Prefix Len</td><td>For IPv4 and IPv6 represents CIDR prefix length of subnet to be allocated from inventory. To assign individual IPv4 addresses to inventory select /32 prefix length.</td></tr>
<tr><td>Available Target Qty</td><td>Once level of inventory of "product assignment" in an available or reserved state is reduced below this value additional addresses are allocated from IP group to new inventory items until inventory level matches target quantity.

Target quantity considers only items previously allocated from this IP Group. Target quantity does not include other items in an available state in inventory created externally to the IP Group.</td></tr>
<tr><td>Active</td><td>When "Yes" allocation from IP Group to inventory is enabled. When "No" allocation to inventory does not occur regardless of inventory levels.

On initial creation if there will be further configuration of allocation requirements it is recommended new allocations be initially set "No" in order to ensure allocation is not able to take place before all intended requirements are fully configured.</td></tr>
</table>

Allocation Requirements

Once an inventory allocation is created one or more requirements may optionally be applied to limit ranges of IP Group from which addresses are allocated.

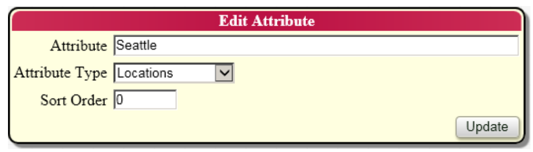


Matching requirements are satisfied either by explicitly matching a range or by matching one or more range attributes. By default when no requirements are configured any inclusive range within the IP Group can be considered for allocation.

If one or more range requirement is specified then to be usable a range must either match corresponding range requirement or one more match attributes have been configured and a range matches all required attributes.

Field	Description
Allow Allocation From Range	Selects a range from the IP group this allocation is able to allocate from regardless of the presence of any range matching attributes.
Require Matching Range Attribute	When one or more range matching attributes are specified a range must match ALL matching attributes of this allocation before the range can be used for allocation. Alternately a range which does not match all attributes may still be used for allocation when there is a match via "Allow Allocation From Range" setting above.

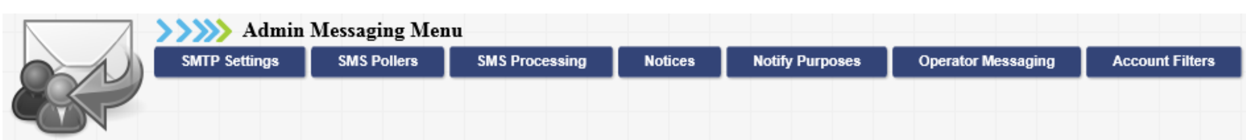
IP Attributes



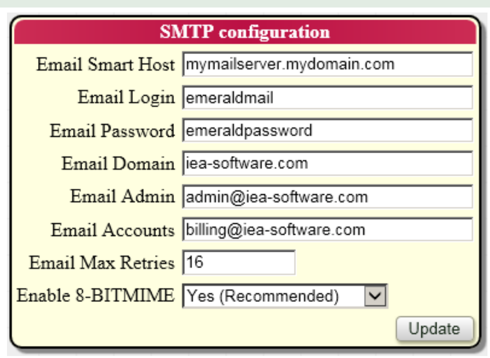
Each attribute represents a fact assignable to one or more ranges of an IP group. Prior to creating attribute click manage attribute types to add categories of attributes. Attribute Types generally represent aspects of an address range such as location, customer type, service level and prefix length. Once attribute types are in place then attributes can be added filling out possible values for each category of attributes.

MESSAGING

Email SMTP settings, SMS server configuration, customer and operator notification is configured from messaging menu.



SMTP



All Email messages are transmitted using Emerald's SMTP client configured here. Before email can be sent SMTP client settings must be fully configured.

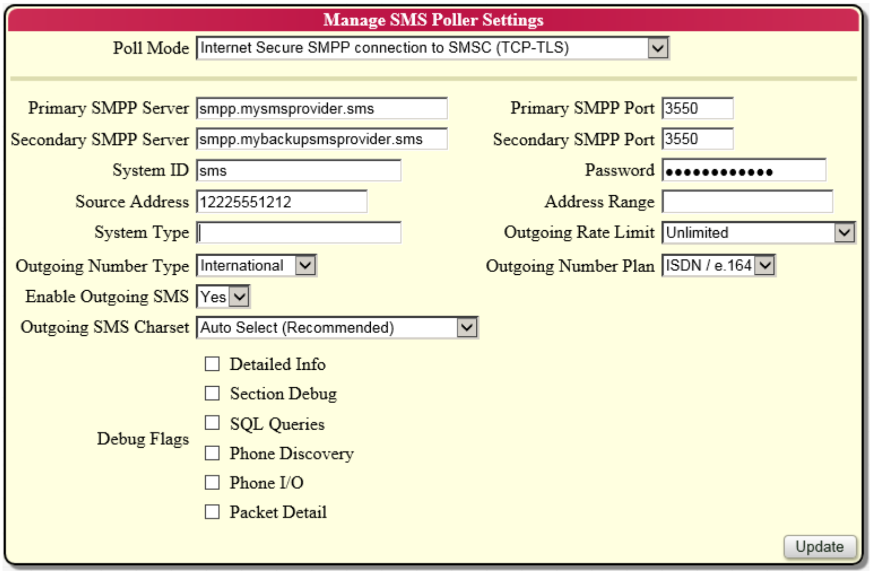
When configuring SMTP take care to ensure either Email account or Emerald server IP Address has been authorized to allow "relay" of mail to external domains.

```
Prior to sending Emails from Emerald please review all Billing Groups to
confirm Email settings including "Email From" address are configured
properly.
```

Field	Description
Email Smart Host	Enter the email SMTP server hostname. By default Emerald connects to SMTP port 25. Alternate ports may be specified by appending ":port" to hostname. For example entering **mymailserver.mydomain.com:587** connects to server mymailserver.mydomain.com using standard TCP submission port 587. Connections to port 465 are assumed to be SMTPS and start as TCP-TLS sessions. Connections to all other ports must begin as cleartext SMTP. When STARTTLS capability is advertised by server connections are always automatically upgraded to TLS.
Email Login	For SMTP authentication this is the login name sent to the SMTP server. Note: CRAM-MD5 and LOGIN auth methods are supported.
Email Password	For SMTP authentication this is the password sent to the SMTP server.
Email Domain	Enter the full email domain name.
Email Admin	Enter the full email address, whereas the value will show in the From: line of all non-accounting related (such as incidents) mailings sent to users.
Email Accounts	Enter the full email address, whereas the value will show in the From: line of all accounting related (invoices and statements) mailings sent to users if billing group specific information is unavailable.
Email Retries	Maximum number of retries for temporary failures before no further delivery attempts is made.
Enable 8-BIT MIME	Enables or disables transmission of 8-bit message body extension field. This should only be disabled to address backwards compatibility with messaging systems unable to process the field. Whether enabled or disabled the content of messages is always transmitted assuming 8-bit.
Certificate Validation	'Disabled' indicates transmission of Email to SMTP server is allowed over clear text TCP as well as STARTTLS and SMTPS without any validation of trust chain. In this mode if STARTTLS or SMTPS is used messages are only secure against passive monitoring. 'Required' indicates secure transmission of Email to SMTP server is mandatory. Clear text SMTP without STARTTLS or SMTPS is disallowed. When using STARTTLS or SMTPS full validation of the certificate trust chain against Emerald's trusted CA database located within emerald/cacerts folder is performed.

SMS Pollers

SMS Poller enables SMS messages to be sent and received from Emerald. Before SMS poller can be used SMS Poller component must be installed using Emerald installer. Poller is not installed by default and will only be included if all modules are installed or SMS Poller module is explicitly selected during Emerald installation.

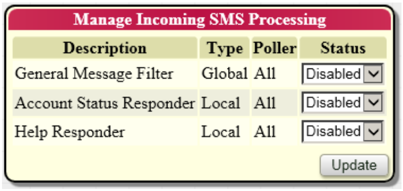


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Poll Mode</td><td>Determines interface and method used to transmit and receive SMS messages.
<table>
<tr><th>Poll Mode</th><th>Description</th></tr>
<tr><td>Internet Secure SMPP</td><td>This mode uses SMPP over TCP-TLS to securely send and receive messages between Emerald and SMSC with mandatory certificate validation.</td></tr>
<tr><td>Internet SMPP</td><td>This mode uses SMPP over TCP to send and receive SMS messages. This mode operates in clear text and is not itself secure.</td></tr>
<tr><td>Serial – Auto Detect</td><td>Detects whether to use poll or listen mode based on GSM modems response to capability queries</td></tr>
<tr><td>Serial – Poll phone storage</td><td>When selected GSM modem is periodically polled for new incoming SMS messages.</td></tr>
<tr><td>Serial – Listen for incoming messages</td><td>When selected incoming SMS messages are sent to the poller as they are received by GSM modem.</td></tr>
</table></td></tr>
<tr><td>Primary SMPP Server</td><td>DNS name or IP address of primary Internet SMPP server</td></tr>
<tr><td>Primary SMPP Port</td><td>TCP port of primary SMPP server. Defaults to standard port 2775 for SMPP and 3550 for Secure SMPP.</td></tr>
<tr><td>Secondary SMPP Server</td><td>DNS name or IP address of backup Internet SMPP server</td></tr>
<tr><td>Secondary SMPP Port</td><td>TCP port of secondary SMPP server. Defaults to standard port 2775 for SMPP and 3550 for Secure SMPP.</td></tr>
<tr><td>System ID</td><td>Username for login to SMPP server</td></tr>
<tr><td>Password</td><td>Password for login to SMPP server</td></tr>
<tr><td>Source Address</td><td>Origination address of messages transmitted to SMPP server. If there is only one address associated with this account source address. This field should be left blank unless instructed otherwise by your SMPP provider.</td></tr>
<tr><td>Address Range</td><td>Address range of destination addresses that should be routed to this SMPP client. This field should be left blank unless instructed otherwise by your SMPP provider.</td></tr>
<tr><td>System Type</td><td>Indicates system type to SMPP provider. This field should be left blank unless otherwise instructed by your SMPP provider.</td></tr>
<tr><td>Outgoing Number Type</td><td>Represents contents of telephone numbers (TON) within Mobile phone field of address records. Any numbers beginning with + are assumed to be international and</td></tr>
</table>

<table>
<tr><td></td><td>transmitted as TON=1 regardless of this setting.
<table>
<tr><th>TON</th><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>International</td><td>Numbers are assumed to be international e.164 standard form including country code and national number.</td></tr>
<tr><td>2</td><td>National</td><td>Numbers are assumed to be in national form (includes area code without country code) as nationally configured within SMPP account.</td></tr>
<tr><td>0</td><td>Unknown</td><td>Number type is not specified. It is up to the configuration of SMPP server account to properly delineate local, national and international numbers contained within mobile phone field of address records.</td></tr>
</table></td></tr>
<tr><td>Outgoing Number Plan</td><td>Represents numbering plan (NPI) within Mobile phone field of address records. It is recommended ISDN / e.164 always be used unless instructed otherwise by your messaging provider. Any number beginning with + are assumed to be international and transmitted as NPI=1 regardless of this setting.
<table>
<tr><th>NPI</th><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>ISDN / e.164</td><td>International e.164 standard numbering plan. This is the recommended setting for all mobile messaging.</td></tr>
<tr><td>8</td><td>National</td><td>Nationally specific numbering plan based on configuration of SMPP server account.</td></tr>
<tr><td>0</td><td>Unknown</td><td>Number plan is not specified. It is up to configuration of SMPP server account to properly select a numbering plan matching mobile phone field of address records.</td></tr>
</table></td></tr>
<tr><td>GSM Modem Port</td><td>When poller is operated in serial mode this option specifies name of serial port to be used for sending and receiving SMS messages. By default "Auto Detect" is selected to enable poller to attempt to automatically detect serial port used by GSM modem.</td></tr>
<tr><td>Outgoing Rate Limit</td><td>If set outgoing SMS messages are rate limited to the selected count within a 10 second window of time. Rate limit normally would only be set if your SMPP provider restricts the transmission rate of outgoing SMS messages.</td></tr>
<tr><td>Enable Outgoing SMS</td><td>When "Yes" transmission of outgoing SMS messages is enabled. When "No" SMS messages may only be received but not transmitted.</td></tr>
<tr><td>GSM Port Settings</td><td>When poller is operated in serial mode this option specifies serial port parameters used to establish communication with SMS modem.</td></tr>
<tr><td>Outgoing SMS Charset</td><td>Provides options for character set conversion from UTF-8 when transmitting outgoing SMS PDUs.
<table>
<tr><th>SMS Charset</th><th>Description</th></tr>
<tr><td>Auto Select</td><td>Character set of outgoing SMS messages will be automatically determined on a per-message basis based on content of message. If message contains characters that cannot be converted to GSM 7-bit character set then entire message shall be converted to Unicode.</td></tr>
<tr><td>Force GSM 7-bit</td><td>Force all outgoing messages to use GSM 7-bit character set. Any characters not part of GSM 7-bit alphabet will be ignored.</td></tr>
<tr><td>Force Unicode</td><td>Force all outgoing messages to Unicode.</td></tr>
</table></td></tr>
<tr><td>AT CMD Timeout</td><td>Length of time from when a serial AT command is issued before abandoning expectation of a response and resetting the poller.</td></tr>
<tr><td>Write Timeout</td><td>Length of time for writes to serial port to complete before the poller is reset</td></tr>
</table>

Debug Flags	When enabled informational and debug level data is written to poller.log file located within Emerald/log folder. It is recommended debug remain disabled normally unless there is a specific need for additional data. Important messages such as information about any errors encountered are always recorded to log file regardless of debug settings.

SMS Processing

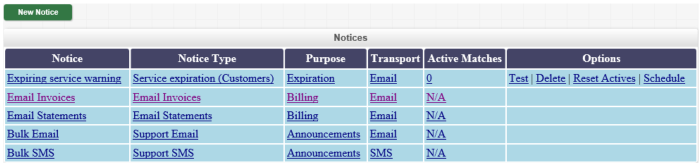


Incoming SMS messages can be filtered and processed for logging or response by enabling processing options configured within this menu. Type may be "Global" meaning the effect of this processing option applies globally before any "Local" type options are executed. When a "Local" processing option is executed its effect is limited to itself and does not affect processing of other options.

Option	Type	Description
General Message Filter	Global	General preprocessing filter to detect and filter out signatures, MMS URIs, forwarded messaging headers and more from incoming SMS message.
*** TBA	Local	Details of SMS processing filters included with future Emerald updates will be displayed here.

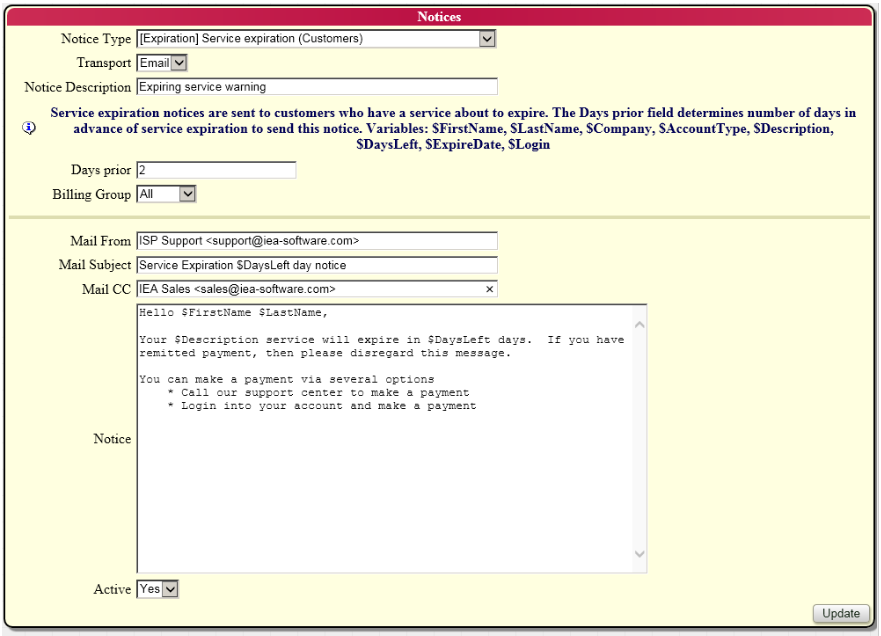
Notices

Email and SMS notification system has a variety of uses including new customer welcome messages, incident status updates, account and credit card expiration warnings, payment receipts, account past due warning, consumption limits and more.



With requisite knowledge of the Emerald system additional types of notifications can be created using Emerald Admin / Advanced / Notice Types menu. Creation of custom notices types is beyond the scope of this document and standard IEA support offerings. Please contact your IEA Software representative about the possibility of implementing custom Email and SMS notifications.

Messages are sent out when the condition of a notice are met. Once the condition the first time and transmission is successful messages are no longer sent until after the condition is no longer met and then reoccurs. As an example we'll use an expired account notice with an expired account having subsequently been paid up and then at some point in the future is expired again. At each point where the account is newly expired a notification would be sent.



Field	Description
Notice Type	The type of notice to be sent. Available notice types appear in the selection list. Once selected a detailed explanation and use instruction is displayed below the notice description field in bold lettering.
Transport	Determines whether notice is to be delivered via Email or SMS
Notice Description	Text uniquely describing the purpose of the email notification
***	Fields specific to a notice type. See notice description of selected notice type for more information.
Mail From	From address of emails sent as a result of the criteria defined here. If Mail From is omitted the billing groups "Email From" field is used.
Mail Subject	Subject of the emails sent as a result of the criteria defined here. If Mail Subject is omitted the billing groups "Email Subject" field is used.
Mail CC	An additional email address to "Carbon Copy" when any emails matching this criterion are sent. If Mail CC is omitted additional copies are not sent.
Mail BCC	An additional email address to "Blind Carbon Copy" when any emails matching this criterion are sent. If Mail BCC is omitted additional copies are not sent.
Attachment Filename	Applicable to Email notices where contents of a notice is a report attached as a file to the notice. Attachment filename enables name of the attached file as it appears in email message to be customized. Variable substitution is allowed within this field. If a file extension is specified as part of attachment filename it is automatically overwritten if necessary to match actual output file format chosen for the attachment. If no file extension is included one is automatically chosen as appropriate. If attachment filename is left blank then the attached report will be named "email" (e.g. email.pdf) Note: This field does not control which report is rendered by this notice.
Default Contact Hours	When transport is SMS field represents default time range describing when notice may send new outgoing messages. Default hours may be overridden by customer specific hours entered with customer contact information. For details on formatting of time range see Common fields.

Notice	Text of the message to be sent as a result of the criteria defined here. The notice description field shown in bold lettering usually contains a listing of "variables" available for replacement in the text of the message sent. Variables allow email messages to be customized for each recipient. Variables can contain items such as Name, Company and account details. An example of the use of variables can be found in the image above. "Hello $Name" is replaced with "Hello Peter" for customers named Peter.
Character Count	When transport is SMS field represents character count of text message.
Active	When active the notice is useable and emails are sent when the Emerald task scheduler executes this notice. When inactive emails are not sent.

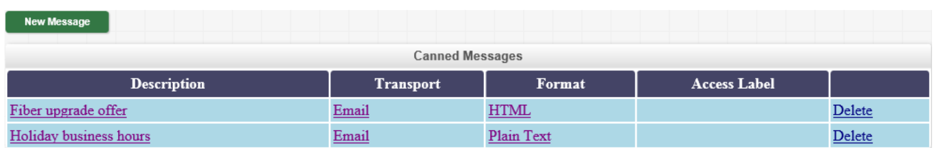
After creating a notice choose the "Schedule" option from the options field of the notices listing to schedule the new notification to run at regular intervals.

"Reset Actives" option should normally never be used. Selecting this causes all accounts currently matching this criterion and having already received a notice to be emailed a second time for the same purpose.

Account Filters

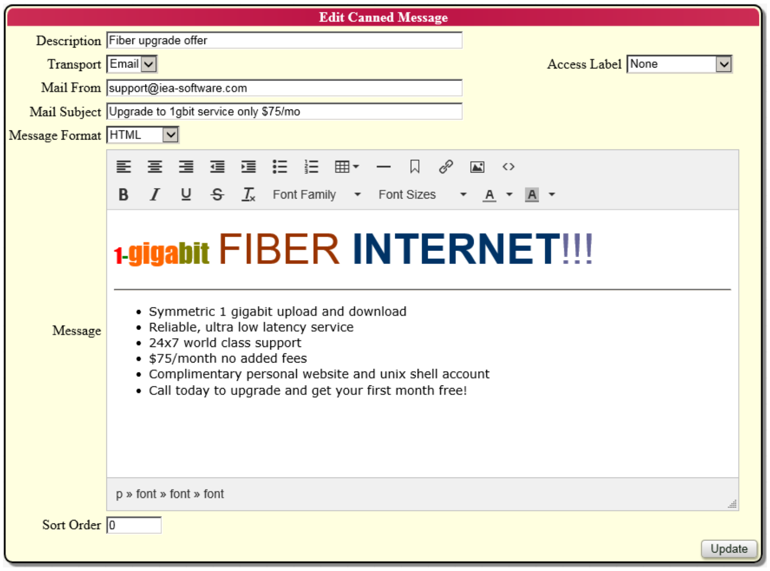
Account filters are used to define customer distribution list criteria when using bulk messaging feature within support menu of Emerald client. For more information please see Account Filters.

Canned Messages



Description	Transport	Format	Access Label	
Fiber upgrade offer	Email	HTML		Delete
Holiday business hours	Email	Plain Text		Delete

Messages expected to be reused as templates for future announcements in conjunction with bulk messaging feature of Emerald support menu are managed here. Examples of canned messages that can be stored are outlines of commonly used maintenance and outage alerts, promotional offers, service changes and news.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Brief text uniquely describing purpose of message. Description appears in the canned message selection list of the bulk email menu of Emerald clients support menu.</td></tr>
<tr><td>Transport</td><td>Determines whether canned message is for bulk messaging via Email or SMS</td></tr>
<tr><td>Access Label</td><td>See Common fields</td></tr>
<tr><td>Mail From</td><td>Prefills from address of bulk emails replacing existing from address if present. If blank the value of from field is unchanged.</td></tr>
<tr><td>Mail Subject</td><td>Prefills subject field of bulk emails replacing existing from address if present. If blank the value of subject field is unchanged.</td></tr>
<tr><td>Message Format</td><td>Regardless of email format selected UTF-8 character encoding is used for all outgoing emails. It is recommended E-Mail servers support 8-bit mime to ensure UTF-8 compatibility.

<table>
<tr><th>Format</th><th>Description</th></tr>
<tr><td>Plain text</td><td>Plain text is universally supported by all mail systems.</td></tr>
<tr><td>HTML</td><td>HTML provides more formatting options vs plain text. When HTML is selected HTML editor interface presented is determined via "Emerald Admin" / "Web Interface" / "Operator Settings" / "HTML Editor".

If none of the included HTML editors are used and HTML tags are entered manually please consider some E-Mail clients support only a small subset of HTML features found in current web browsers when rendering HTML formatted email messages.</td></tr>
</table></td></tr>
<tr><td>Message</td><td>Body of Email or SMS message to be used as a template for bulk messaging.

The following variables substitutions per table below are supported within message body of SMS and Email messages. Following example demonstrates customizing each message with name of MBR billing contact.

Hello $FirstName $LastName,
…
…
…</td></tr>
</table>

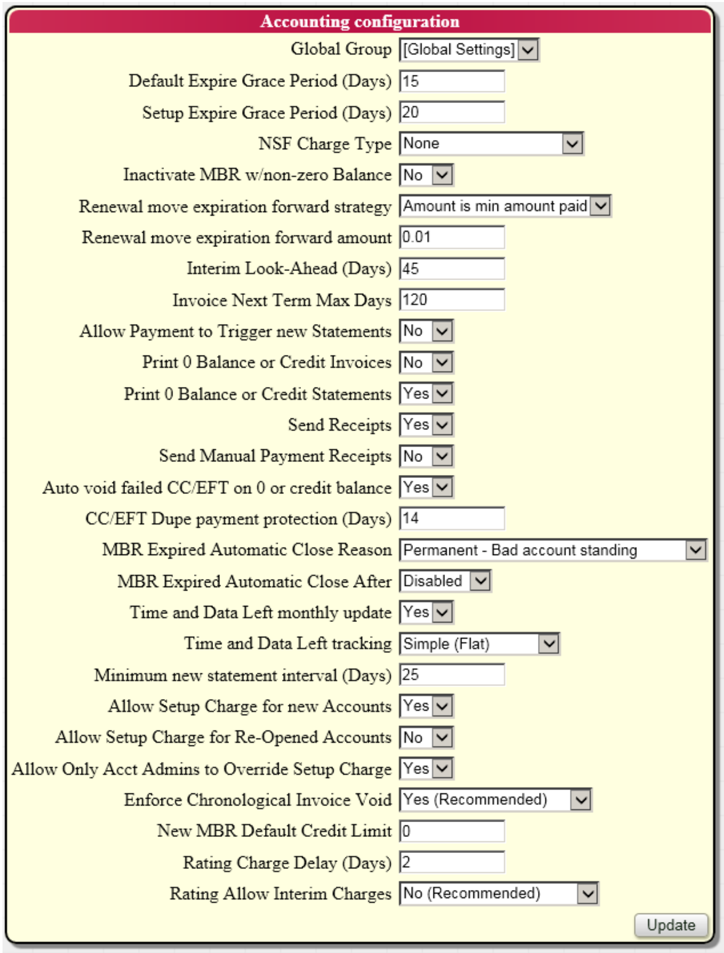
	Variable	Description
	$FirstName	Last Name field from primary billing address of MBR
	$LastName	First Name field from primary billing address of MBR
	$Company	Company field from primary billing address of MBR
	$CustomerID	MBR # (Customer ID)
Sort Order	See Common fields	

ACCOUNTING

Emerald billing and payment processing related configuration is managed from this menu. Options include billing settings, charge types, pay periods, taxes, billing cycles, send methods, GL codes, CC/EFT batch processing, late fees, time & data charges, payment types and plans.

Settings

Billing and related account options are controlled from settings menu. Settings can be applied globally for all accounts or separately by billing group.



Field	Description
Global Group	When a billing group is selected accounting settings are configured separately by billing group. Once configured an '*' appears before the group name indicating the groups configuration is not the same as global group.
Default Expire Grace Period (Days)	Sets the default permanent extension when creating a new service. Note that the default expire grace period is overridden by "Default Extension (Days)" setting of the billing cycle assigned to the MBR.
Setup Expire Grace Period (Days)	Sets the temporary extension field in the MBR to allow an initial one-time grace period on initial account creation. After the MBR is invoiced the temporary extension value is removed from the MBR.
NSF Charge Type	Charge type to be used when necessary to bill non-sufficient funds charge to an account when payment is dishonored from MBR payments menu.
Inactivate MBR w/non-zero Balance	When set "Yes" allows canceled MBRs to be inactivated regardless of accounts remaining balance. When set "No" accounts balance must first be settled before a canceled account will automatically be marked inactive. Note for recurring billing cycle types "Inactive" accounts do not count against licensed MBR count.
Renewal move expiration forward strategy	These options control how much of an invoice line item needs to be paid for recurring services before the expiration date is set to the accounts billed thru date. These settings apply only to renewal billing cycles.

<table>
<tr><td></td><td>
<table>
<tr><th>Strategy</th><th>Description</th></tr>
<tr><td>Amount is min amount paid</td><td>When chosen the amount field below is the minimum amount that must be paid against a given invoice line item before the expiration date is advanced to the billed thru date regardless of the total cost of the line item.</td></tr>
<tr><td>Amount is min percent paid</td><td>When chosen the amount field below is the minimum percentage of the invoice line item that must be paid before the expiration date is advanced to the billed thru date.</td></tr>
<tr><td>Proportional to payment</td><td>When chosen then expiration date is advanced proportional to the percentage of the invoice line item that has been paid. For example assuming 50% of a monthly recurring account has been paid the expiration advances 15 of the 30 days in a given month.</td></tr>
<tr><td>Full payment required</td><td>When chosen the invoice line item must be paid in full before the accounts expiration date is advanced to match the billed thru date.</td></tr>
</table>
</td></tr>
<tr><td>Renewal move expiration forward amount</td><td>This field is used with the ‘Renewal move expiration forward strategy’ option above. This field is required when using the ‘Amount is min amount paid’ or ‘Amount is min percent paid’ options. The field is not used when ‘Proportional to payment’ or ‘Full payment required’ is chosen.</td></tr>
<tr><td>Interim Look-Ahead (Days)</td><td>This feature is designed to prevent unnecessary invoicing of accounts with long duration pay periods. When an adjustment or charge is made against an account and the MBR is not due to be invoiced again for recurring services within the "Interim Look-Ahead" days an interim invoice can be created for unapplied charges. If an invoice for recurring services is scheduled on or before "Interim Look-Ahead" days the creation of the interim invoice is delayed so that the unapplied charges or adjustments are made to appear on the same invoice as recurring charges.</td></tr>
<tr><td>Invoice Next Term Max (Days)</td><td>Operators have the ability to manually force invoicing of accounts into the future beyond "invoice bill days" defined at the billing cycle level. This option places a limit on how far services can be billed thru into the future while still allowing operators to manually force invoice creation for the accounts next term.</td></tr>
<tr><td>Prorate of less than (Days) adds following month</td><td>While invoicing for a month and service is prorated such that only a small fraction of the month period is invoiced this setting determines whether to include a following month of service.

For example invoice is created for a month of service. It normally contains a prorated line item covering only 5 days out of the monthly billing period.

If this setting is 6 or more than the above invoice would also include the following month of service in addition to the 5 days for a total of 1 month 5 days of service.

If this setting is 5 or less in the same scenario the invoice would cover only 5 days of service. The following month would be billed separately on a subsequent invoice.</td></tr>
</table>

	This setting applies only to services with monthly pay periods. For pay periods covering multiple months the maximum effective value is 4.
Reinvoice Invoice Void Limit (Count)	While reinvoicing an MBR should more than set number of invoices be voided as a result of a single reinvoice operation then reinvoice processing fails. Limits are intended primarily to prevent accidental entry of wrong data into timeline resulting in widespread unintended automatic voiding of prior invoices. If empty or 0 then no reinvoicing limits are applicable. When -1 no invoices can be voided by reinvoice. If there is a special need to override this limit it is recommended operators void latest recurring invoices manually prior to reinvoice. This effectively results in reduced number of remaining void steps during reinvoice allowing count of voided invoices to fall within allowed range.
Allow Payment to Trigger new Statements	When enabled any payment applied to an MBR is eligible to cause the creation of a new statement subject to standard restrictions including minimum new statement interval and invoicing lookahead window. It is recommended this feature be set "No" to prevent payments from triggering creation of new statements. This feature has the potential to delay statements triggered by new invoices should they fall within the minimum new statement interval yet outside the invoice lookahead window.
Gapless Invoice Numbering	When "Enabled" any gaps appearing in sequential numbering of invoices for any reason including aborted invoice transactions, canceled POS invoices and estimates or database specific sequence pooling are retroactively filled in by new future invoicing activity to ensure no gaps exist in sequencing of invoices. When "Disabled" any gaps in invoice sequences are ignored and no attempt is made to retroactively fill in missing invoice numbers in sequence. It is recommended this setting remain disabled unless there is a specific need for gapless invoice numbering. When enabled scheduled task "Gapless invoice numbering data collector" periodically gathers gap data to be used during new invoice creation.
Credits reduce taxable amount	When "Enabled - Within Invoice" a credit rolled into the same invoice as taxable charges reduces taxable amount of charges within the invoice until credit amount is exhausted. When "Disabled" a credit rolled into an invoice has no effect on the taxable amount of line items within the invoice.
Check / CC / EFT Payment Fee	Enables MBRs to be charged a per-transaction processing fee whenever payments of chosen payment type are accepted. Fee is static amount configured at charge type level applicable to all MBRs globally or by billing group regardless count of payments accepted within a given time or amount of each payment. This feature applies only to recurring MBRs. MBRs with non-recurring billing cycles are not charged payment fees. Additionally once an MBR has been temporarily or permanently canceled the fee is no longer

	applied to subsequent payments while MBR remains canceled in order to facilitate settlement of outstanding balances. While payment fee is normally applied globally or by billing group the fee can be discounted or waived entirely via configuration of charge type auto assign market tags. Operators may also manually waive fees by deletion of unapplied adjustments from MBR invoices menu.
CC Payment Fee (Percentage)	When a CC payment charge type is selected this represents an optional fee cost in addition to static amount of charge type as percentage of payment amount. For example if CC Payment Fee charge type has static amount of 1.00 and percentage is "10" then for a credit card payment of 200.00 the total fee amount is 1 + 20 = 21.00. When 0 or left empty no additional amount above charge type static cost is applicable. When nonzero and a CC Payment Fee charge type is not selected this setting is ignored and no fee is applied.
Email 0 Balance or Credit Statements	When "Yes" statements with will be emailed to the customer regardless of balance. When "No - Current Balance" statements will not be emailed to the customer if the ending statement balance is 0 or credit amount. When "No - *** Day Balance" statements will not be emailed to the customer if the corresponding statement aging bucket or higher has a balance of 0 or credit amount.
Email 0 Balance or Credit Invoices	When "Yes" fully paid invoices will be emailed to the customer.
Print 0 Balance or Credit Statements	When "Yes" statements with will be included in batch printing for mailing to the customer regardless of balance. When "No - Current Balance" statements will not be mailed to the customer if the ending statement balance is 0 or credit amount. When "No - *** Day Balance" statements will not be mailed to the customer if the corresponding statement aging bucket or higher has a balance of 0 or credit amount.
Print 0 Balance or Credit Invoices	When "Yes" fully paid invoices will be included in batch printing for mailing to the customer.
Send Receipts	When "Yes" payment receipts for new payments are automatically emailed to the customer. When "No" the customer can obtain receipts from the Customer interface or an Operator can manually send a payment receipt. Customer can disable receipt of payment receipts by disabling Account status notifications from the customer interface.
Send Manual Payment Receipts	When enabled receipts are sent for payments made manually by Emerald operators. When disabled receipts are only sent for automatic CC or EFT transactions.
CC/EFT auto pay for POS Invoices	This setting manages whether MBRs configured for CC/EFT auto pay should also auto pay POS invoices. This setting is for POS invoices generated by operators only. Setting does not apply to Customer POS invoices managed from the customer account center and does not apply to POS invoices with an assigned payment plan. **Option** | **Description**

	<table><tr><td>Disabled</td><td>When an MBR is configured with pay method of Credit Card or Bank Transfer the presence of unpaid POS invoices will neither trigger creation of a CC/EFT autopay transaction nor add to the transactions amount. This mode requires POS invoices either be configured with a payment plan or paid manually even when the customer is configured for CC/EFT autopay.</td></tr><tr><td>Enabled</td><td>When an MBR is configured with pay method of Credit Card or Bank Transfer the presence of unpaid POS invoices shall both trigger creation of a CC/EFT autopay transaction and add to the transactions amount. Presence of a payment plan for a POS invoice takes precedence over this setting. If a payment plan is used then this setting is treated as 'Disabled' for that POS invoice.</td></tr><tr><td>Add Unpaid</td><td>When an MBR is configured with pay method of Credit Card or Bank Transfer the presence of unpaid POS invoices does not trigger creation of a CC/EFT autopay transaction however if a CC/EFT transaction is generated to pay other invoices within the MBR then at that time transaction value is increased by unpaid amounts of POS invoices. If more than a month has passed and POS invoice remains unpaid then presence of unpaid POS invoice shall trigger the creation of a CC/EFT autopay transaction. This setting is intended to combine a customer's monthly recurring invoice related CC/EFT autopay transaction with any POS invoices occur within preceding month into a single CC/EFT transaction. This differs from 'Enabled' in that with enabled presence of POS invoice causes auto pay transaction to be generated right away to cover the POS invoice rather than waiting for subsequent recurring invoice to occur. Presence of a payment plan for a POS invoice takes precedence over this setting. If a payment plan is used then this setting is treated as 'Disabled' for that POS invoice.</td></tr></table>
Auto void failed CC/EFT on 0 or credit balance	When "Yes" any failed automatic transactions within an MBR are automatically voided when the MBR has a zero or credit balance.
Allow CC/EFT New Payment Void (Hours)	Determines number of hours after a Credit Card or EFT transaction is successfully completed a transaction may still be voided from within Emerald. Once the period has elapsed the ability to void transaction is replaced with option to issue a credit against the payment. This period should coincide as much as possible with approximate

<table>
<tr><td></td><td>timing of credit card settlement procedure. If an operator attempts to void a transaction having already settled the void operation fails and it becomes necessary to wait for void hours to elapse before operator is given opportunity to issue a credit</td></tr>
<tr><td>CC/EFT Dupe payment protection (Days)</td><td>This is a safeguard preventing CC or EFT transactions of the same amount from being processed within configured number of days. If a duplicate transaction is detected when adding a payment operator is prompted with a dialogue asking if they would like to continue anyway. If the duplicate payment is an automatic transaction it is marked as waiting to be confirmed. These transactions can be confirmed or voided from the Batch / Failed Transactions menu.</td></tr>
<tr><td>Recurring MBR Expired Auto Close Reason</td><td>When automatically closing an MBR with a renewal billing cycle this specifies the cancellation reason associated with the automatic closure.</td></tr>
<tr><td>Recurring MBR Expired Auto Close After</td><td>Period of time after which all services within an MBR with a renewal billing cycle have expired to automatically close the account. Note the scheduler task ‘Expired MBR Auto Close’ must be enabled.
See Scheduler / Configure schedule.</td></tr>
<tr><td>Non Recurring MBR Expired Auto Inactivate After</td><td>Enables the automatic inactivation of MBRs with a nonrecurring billing cycle when one or more services are expired and the latest service expiration was reached more than selected days ago. It is normally recommended this setting remain disabled to allow returning customers to reuse their existing accounts.

This feature does not apply to nonrecurring MBRs with no services or where no services expire.

Note the scheduler task ‘Expired MBR Auto Close’ must be enabled.
See Scheduler / Configure schedule.</td></tr>
<tr><td>Time and Data Left nonrecurring purchases</td><td>Determine how purchased blocks of time and data are to be integrated with a services existing time and data allocation. This setting is only applicable when all of the following conditions are satisfied.

• Service is non-recurring
• Time and data left tracking setting below is Simple (Flat)
• Service is currently time or data limited
• New block of time or data purchased via POS invoice
• Service is expired at time POS invoice is fully paid

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>If expired replace existing time and data</td><td>If service has an existing quantity of time and purchased block provides a quantity of time services existing time remaining is reset to match purchased block. This occurs regardless of whether existing time remaining is more or less than purchased block or has a negative value.

The same applies to purchased blocks of data or rating time and rating data.</td></tr>
<tr><td>If expired add to existing time and data</td><td>If service has an existing positive quantity of time and</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td></td><td>purchased block provides a quantity of time then the purchased blocks time is added to existing time.

If the service has a negative quantity of time and purchased block provides a quantity of time then the services existing time remaining is set equal to purchased block of time.

The same applies to purchased blocks of data or rating time and rating data.</td></tr></table></td></tr>
<tr><td>Time and Data Left tracking</td><td>This option controls how time and data left usage limits are consumed and tracked. This option can be changed without affecting the time/data currently allocated to existing accounts.

<table><tr><th>Tracking</th><th>Description</th></tr><tr><td>Simple</td><td>The time and data left fields in the service are incremented when additional time is added via one-time charges or direct use prepaid cards. This allocation never expires although the account itself may expire based on expiration date.

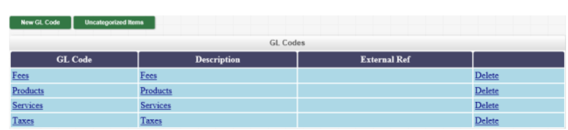
How existing service time and data left allocations are treated when additional blocks of time are purchased for an existing expired service is conditioned upon "Time and Data Left nonrecurring purchases" setting above.

For recurring accounts with ‘time/data left monthly update’ enabled additional time is only added by the monthly time/data left replenishment process if current value of time/data left is less than the monthly allocation or rollover accumulation limit. If an invoice containing a one-time usage line item that has incremented time left or data left in the service then voiding that invoice does not change that allocated time or data remaining.</td></tr><tr><td>Detailed</td><td>When enabled time and data purchased via one time charges or direct use prepaid cards are tracked separately outside of the time left and data left fields displayed when editing a service. While the service time/data left fields are not affected by one-time/direct use time/data purchases their value in the service field must not be blank if any such limits are to be enforced. If expiration Month/Day/Minutes are set via the one-time charges menu the purchased time expires after the combined months/day/minutes limit has passed. Similarly for direct use prepaid cards active expire days field controls length of time the prepaid time/data is available for consumption. For recurring accounts with ‘time/data left monthly</td></tr></table></td></tr>
</table>

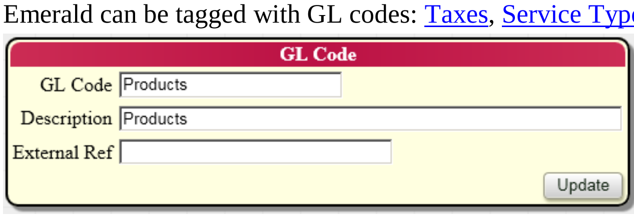
	update' enabled the monthly time and data allowances are reset in the time left field at the start of the customers new monthly period. Any additional purchased time/data is used only after the monthly allowances are consumed in reverse chronological order. For example customer "neila" has a recurring account providing 1000 minutes of access per month. A few days before the start of his next month he runs out of time and purchases 5000 additional minutes. He uses 200 of them before the next month starts. The remaining 4800 minutes purchased are available in subsequent months and consumed only after that month 1000 minutes are exhausted. If an invoice containing purchased time is voided the associated allocation of time/data usage is also removed.
Time and Data Left monthly update	When "Yes" remaining time and data in a services time left and data left fields are updated once a month provided a default time or data left is configured for the accounts service type and services time or data left field is not blank or greater than its current rollover value. When "No" Automatic monthly updating of time and data left fields is disabled.
Minimum new statement interval (Days)	Controls minimum allowed interval between automated statement creations. This setting is intended to prevent too many statements from being created for an account based on activity in a given period. If interval is configured too low it may allow multiple statements to be sent unnecessarily to the customer within a billing month. If interval is too high delivery of new charges based on recent invoicing activity may be delayed. Recommended default new statement interval is 25 days for once a month delivery. In conjunction with the invoicing lookahead interval this setting enables statement timing to quickly "settle" into the optimal timing. While statements can be manually created for an MBR at any time regardless of statement interval this practice is strongly discouraged when using a minimum new statement interval intended to limit statement creation to one statement per month. This is because one off statements created manually at the wrong time means minimum new statement interval (for example 25 days) must pass before the system can create a statement manually. If created at the wrong time this can lead to excessive delay between creation of invoice for new charges and subsequent statement delivery to customer.
Allow Setup Charge for new Accounts	When "Yes" any applicable setup charge is available to be applied when opening a new account. When "No" no setup charge is applied for new accounts.
Allow Setup Charge for Re-Opened Accounts	When "Yes" any applicable setup charge is available to be applied when re-opening a preexisting account. When "No" no setup charge is applied for re-opened accounts.
Allow Only Acct Admins to Override Setup Charge	When "Yes" only Operators of operator groups having the MBR Acct Admin object group assigned or global administrators may override the default setup charge settings. When "No" any operator may override the default setting.

Allow ‘Custom’ Charge Type for Adjustments	When "Yes" the custom charge type is selectable to operators when creating a new adjustment or POS invoice. When "No" the custom charge type is not selectable. Enabling this option may be useful to prevent operators from applying custom charges or credits to accounts that are not categorized into proper GL Categories for accounting purposes.
Enforce Chronological Invoice Void	When yes the billing system requires that any voided invoice containing recurring line item be voided in chronological order from newest to oldest so that proper adjustments can be made to the billed thru dates of affected services. It is highly recommended this be enabled. If it becomes necessary to disable this feature to address a specific account we recommend re-enabling this as soon as possible after making changes to the account.
New MBR Default Credit Limit	Default amount to set in the credit limit field while creating a new MBR with a balance forward billing cycle type.
Rating Charge Delay (Days)	Number of days after the rating summaries monthly period has elapsed before creating a charge for usage based on the summary. The delay is intended to provide some additional time for accounting data from the previous month to close out the month’s usage in a single charge. If additional accounting data for a previous monthly period arrives after the delay period the system will generate an additional charge to account for any late arriving accounting data.
Rating Allow Interim Charges	When "Yes" charges will be created against any currently rated data regardless of whether the monthly period covered by the rated data has passed each time usage charges are processed. A setting of "Yes" is not recommended as it may cause many usage charge line items to appear on a single invoice or multiple invoices to be created when they would not otherwise. This is useful only if you need to invoice customers for their data usage on smaller intervals without having to wait for their monthly period to end. When "No" charges for rated data are only created after the period covered and the Rating Charge Delay above has passed. "No" is the default and recommended setting.

GL Codes



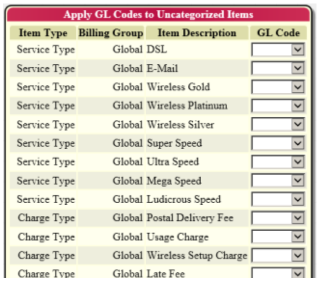
GL codes offer a means of associating billing information in Emerald to the general ledger categories of your organization's accounting system. The following billing related items in Emerald can be tagged with GL codes: Taxes, Service Types, Payment Types and Charge Types. Once GL codes have been assigned GL related reports including GL invoiced for accrual or GL payments for cash basis can be used to provide summary inputs into an accounting system.



Field	Description

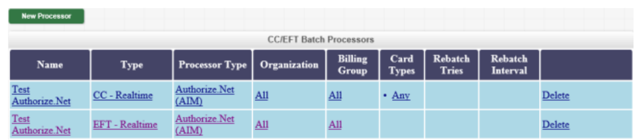
GL Code	An identifier for the GL Code typically matching up with an identical identifier configured within accounting system. This will be sent to the accounting system with each export entry.
Description	Additional details related to GL Code.
External Ref	See Common fields

Uncategorized Items

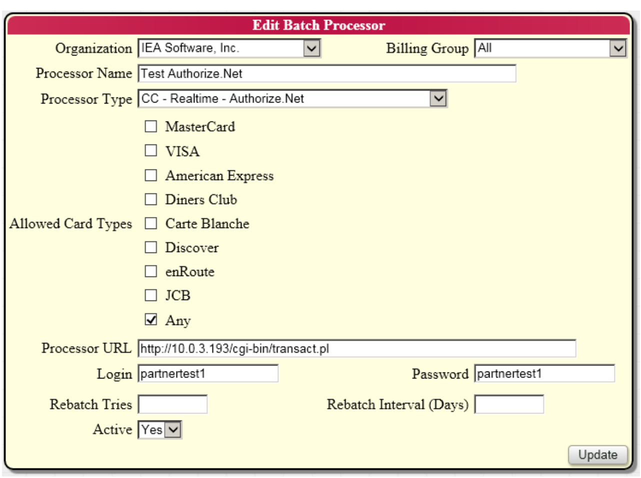


This submenu option of GL Codes offers a unified view of any Service Types, Charge Types, Taxes, Tax Sources and Payment Types where a GL Code has not yet been assigned. To associate GL Code with one or more items select GL Code from the list corresponding with item. Once a GL Code has been assigned item shall no longer be visible from Uncategorized Item list. If you wish to change a GL Code for an item where GL Code has already been assigned in the future you may do so by updating configuration item directly from corresponding Administrative menu within Emerald.

Batch Processors



Credit Card and EFT processing is handled through the configuration of batch processors. Configuration of a batch processor determines both interface used to communicate with an external batch transaction system and also internal criteria used in the selection of an appropriate batch processor such Organization, Billing Group and accepted credit card brands.



Field	Description
Organization	Organization the batch processor is to be used with. Each organization separately processing credit card and EFT transactions must have its own batch processor defined.
Billing Group	Optional billing group to further restrict the use of this batch processor. Note "All" billing group includes only those billing groups assigned to the selected Organization.

<table>
<tr><td>Processor Name</td><td>Text describing the purpose and use of this batch processor. Processor name appears in the "Credit Card" and "Bank Trans" options of the "Client" / "Billing" menu.</td></tr>
<tr><td>Processor Type</td><td>Specifies the transaction system to be used for CC or EFT processing. Please contact your sales representative about the possibility of supporting additional processors if you would like to use a transaction gateway not listed here.

<table>
<tr><th>Processor Type</th><th>Description</th></tr>
<tr><td>Batch</td><td>Credit card and EFT interfaces relying on periodic manual batch file exports for processing by external software.

Export file is provided to external processor. Once processing is completed a result file is typically imported back into Emerald in order to record both accepted and failed transactions and credit accounts accordingly.

Batch based processors are not commonly used due to processing delays and need for manual intervention. Batch based processors are included primarily for backwards compatibility and should generally be avoided in favor of real-time processing.</td></tr>
<tr><td>Realtime</td><td>Enables credit card transactions to be immediately transmitted to remote processing gateway typically over Internet for immediate consideration providing both operators and customers using customer account center with real-time feedback on the status of their payment transaction.

Note while EFT transactions using real-time gateways are transmitted from Emerald in real-time they do not block funds like credit cards and so there is no assurance EFT transaction will ultimately succeed. Upon failure the operator is notified by bank of NSF or other condition and must manually dishonor associated payment within Emerald to reflect that payment was not accepted.</td></tr>
<tr><td>Tokenized</td><td>Operates similar to real-time processors except credit card account numbers are stored within the remote processing gateway rather than within Emerald to limit liability in the event of data breach. Instead "tokens" which are a unique representation of a card account number known only to the gateway are stored and used for future processing of CC transactions.

When a tokenized batch processor is selected additional options appear in the batch processor listing to support tokenization of existing stored cards as well as a de-tokenization feature to reverse the process are provided. Please follow on screen instructions carefully when using these features.</td></tr>
</table></td></tr>
<tr><td>Allowed Card Types</td><td>When used with a credit card gateway allowed card types menu allows you to define all credit card types you wish to accept. For example if you accept Visa and MasterCard but do not accept Amex or a different processor handles Amex you would check "MasterCard" and "Visa" leaving Amex unchecked. The "Any" option allows all types of credit cards to be accepted by this batch processor including card types not explicitly listed.

If credit card account numbers are manually imported from external systems by data</td></tr>
</table>

	import and card statistics were not configured selecting "Any" will allow processing of transactions where otherwise processing would fail due to card types of imported card types not being properly configured.
Processor URL	When used with a network based "Processor Type" processor URL is generally an HTTPS URL of the provider's transaction web service. For non-web service oriented "Processor Types" the Processor URL reflects the network address of the processing system in the form "IPAddress:Port". When a processor type is selected the most common processor address will automatically be entered into the Processor URL field. It is recommended this default not be changed unless you have been specifically requested to. For security always use https:// URLs instead of http:// for production use to protect card account numbers transmitted over the network.
Login (Varies)	When a network based "Processor Type" is selected the login field represents the access account name or ID used to identify your organization to the transaction processing service.
Password (Varies)	When a network based "Processor Type" is selected the password field represents the access password or secret key (Transaction key) used to authenticate the identity provided above to the transaction processing service.
Batch Out File	When a file based "Processor Type" is select the batch out file represents the file(s) all credit card transactions Exported from Emerald are written to. The batch out file is generated locally from the perspective of the system running the Emerald task scheduler.
Batch In File	When a file based "Processor Type" is select the batch in file represents the result file(s) generated by the transaction processing software. The batch in file is read locally from the perspective of the system running the Emerald task scheduler.
Export Options	When a file based "Processor Type" is selected this Indicates what the system should do with the export batch file(s) if they already exist before performing an additional export.
Import Options	When a file based "Processor Type" is selected this Indicates what the system should do with the import batch file after it has been successfully processed.
Batch Limit	When a file based "Processor Type" is selected batch limit provides a limit on the number of transactions that can be exported at any one time to the export file.
Rebatch Tries	Enter the number of times that some types of failed transactions can be automatically retried. Only transactions created automatically via MBR payment types of "Credit Card" or "Bank Transfer" can automatically be retried. Manually submitted transactions which fail must be manually re-submitted.
Rebatch Interval (Days)	Enter the number of days to wait between each "Rebatch Try" configured above.
PAN Backup Certificate	When using a tokenized processor backup certificate allows account numbers to be safely stored so that tokenization process may be reversed in the future without relying on processor to provide account number data necessary to reverse tokenization. Stored account numbers are encrypted with chosen backup certificates public key. To maintain benefits of tokenization private key required for decryption is never stored within Emerald. Changes to backup certificate configuration impact entry of new card numbers from the point of change forward and have no effect on prior data.
Active	When a batch processor is Active transactions are assignable to it. When a batch processor is Inactive new transactions are no longer assignable to that batch processor however any existing assigned transactions will continue to be processed normally regardless of the "Active" status.
Merchant ID (Varies)	Option visible only when the "Processor Type" requires or can accept an optional Merchant ID provided by your transaction processing company.
Store (Varies)	Option visible only when the "Processor Type" requires or can accept an optional Store provided by your transaction processing company.

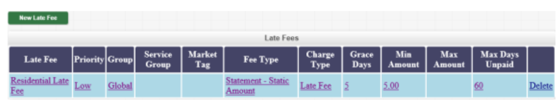
Terminal (Varies)	Option visible only when the "Processor Type" requires or can accept an optional Terminal provided by your transaction processing company.

If multiple batch processors are defined Emerald selects the most specific batch processor matching all criteria able to process the transaction. Following ranks batch processors in order of most to least specific.

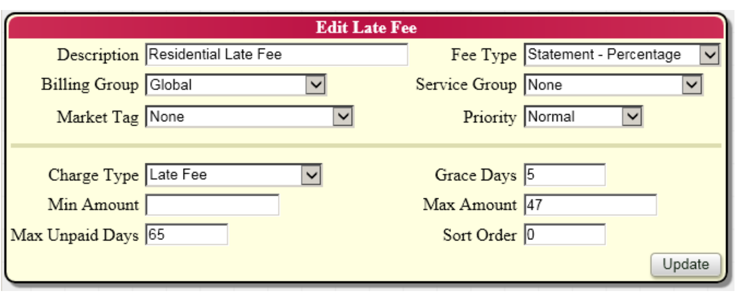
- Billing group match of a tokenized CC processor
- Billing group match where allowed card type also matches excluding "Any"
- Billing group match of EFTs or CC where allowed card type is "Any"
- Organization match of a tokenized CC processor
- Organization match where allowed card type also matches excluding "Any"
- Organization match of EFTs or CC where allowed card type is "Any"
- Global match of a tokenized CC processor
- Global match where allowed card type also matches excluding "Any"
- Global match of EFTs or CC where allowed card type is "Any"

```
When creating a batch processor for use with new Authorize.Net accounts take
care to choose the Authorize.Net real-time processor type ending with "(AIM)"
```

Late Fees



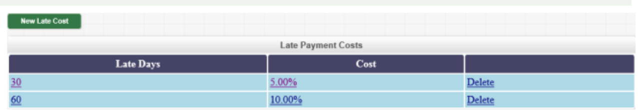
Late fees provide an ability to issue monetary penalties for customers with an outstanding balance for an extended period of time. Late fees can be a fixed amount or percentage and may change over time depending on customer delay in transmitting payment. Assessment of late fees is delayed until either the "Max Unpaid Days" limit configured within the late fee is reached or late payment is finally received. If payment is received and marked with a receive date earlier than the payment is applied the receive date shall be honored as long as Max Unpaid Days has not already passed and a late fee already created.



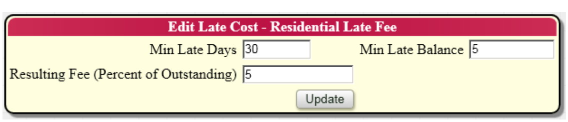
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Text describing the purpose and configuration of the late fee.</td></tr>
<tr><td>Fee Type</td><td>Determines how to assess fee in terms of percentage unpaid or static fee and whether fee is applied to unpaid line items or to the statement.
<table>
<tr><th>Fee Type</th><th>Description</th></tr>
<tr><td>Statement - Static Amount</td><td>Late fee will be a static amount based on payment status of all items of statement.</td></tr>
<tr><td>Statement - Percentage</td><td>Late fee will be a percentage amount of all unpaid items of statements.</td></tr>
<tr><td>Line Item - Percentage</td><td>Late fee will be a percentage amount of all unpaid line items of the MBR.</td></tr>
</table></td></tr>
</table>

Billing Group	If set late fee is restricted to only MBRs with matching billing groups
Service Group	If set late fee is restricted to only MBRs with a billing group that is a member of matching service group
Market Tag	If set late fee is restricted to only MBRs where selected MBR level market tag is active
Priority	Since only a single late fee may be assigned to a MBR in the event multiple late fees match priority is used to help select the best matching late fee. Matching fee with the highest priority is selected. If more than one late fee has same priority then the lowest sort order late fee is used.
Charge Type	Charge type used in assessing the late payment fee. The line item description of the late fees on the customers invoice is based on the description of the charge type rather than the description of the Late Fee itself. Any taxes applied to the charge type also apply to the late fee.
Grace Days	Number of days from statement due date or line item start date allowed to pass before min late days within a late cost begins to accumulate. For example if Statement was due 30 days ago and Grace days is 5 a late cost of 30 days will match in the future when Statement is due 35 days ago.
Min Amount	The minimum possible amount of the late fee to be charged if there is any outstanding balance covered by a late payment cost.
Max Amount	The maximum possible amount of late fee to be charged.
Max Unpaid Days	Represents maximum number of days a line item or statement may go unpaid before a late payment charge adjustment is applied. Max Unpaid Days should be set higher than any late costs configured within this late fee.
Sort Order	Secondary sort for determining applicable late fee after priority. Also see Common fields
Active	When "Yes" this late fee can be selected for applying late payment fees to MBRs. When "No" this late fee is not considered for application of late payment fees to MBRs. Setting a late fee inactive does not prevent other lower priority active late fees from being applied in place of the inactivated late fee.

Late Costs



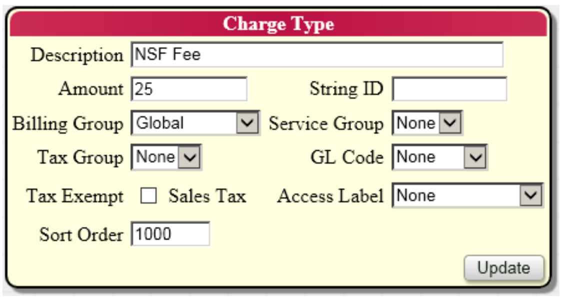
Once the late fee is created a menu option appears to add late costs to the fee. Late costs define amount of the fee based on minimum days late payment is. Any number of late costs may be assigned to a late fee to provide an escalating fee schedule. When accessing fees system choses the highest late cost that meets minimum criteria of the last cost.



Field	Description
Min Late Days	Minimum number of days past grace needed for this late cost to apply
Min Late Balance	Minimum remaining balance on statement or line item depending on fee type for the late cost to apply
Resulting Fee	Percentage or static amount of outstanding balance to charge when minimum late days and balance of this late cost have been reached

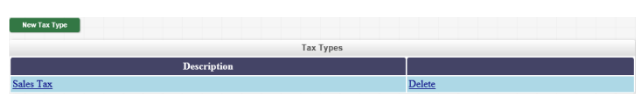
Charge Types

Charge Types define types of non-recurring charge adjustments able to be manually or automatically applied to an MBR. These charges are typically one-time fees for a service (Setup fees, product and service sales, late fees, usage fees, NSF fees, ETF fees, send method charges and more) Charge Types also define any applicable taxes, GL Codes and are available for selection when creating an adjustment or POS invoice within a MBR.



Field	Description
Description	Enter an identifying description for the Charge Type. This entry will be presented within the 'Charge Type' selection lists throughout Emerald.
Amount	Enter the default charge amount for this charge type. The Amount can be a credit or a debit entry. This default can be over-ridden within the Adjustment entry screen.
String ID	See Common fields
Tax Group	Choose the default Tax Group for this Charge Type. Defining a Tax Group indicates the Tax Group that should normally be applied to this type of account charge. The Tax Group default can be over-ridden on the account adjustment screen.
Tax Exempt	Enabling a tax exemption indicates any applicable taxes with a matching exemption are not applicable to invoice line items involving this charge type.
Access Label	See Common fields
Billing Group	Restricts charge type's availability to selected billing group
Service Group	When configured in addition to selected billing group the charge type is also accessible to service groups that include "Charge Types".
Sort Order	See Common fields
GL Code	GL Code applicable to any line items based on this charge type.

Tax Types

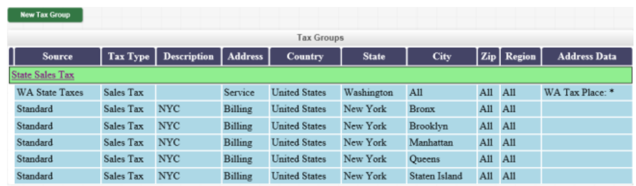


Each kind of tax to be charged should be configured as a tax type. Examples of tax type include Sales Tax, regulatory fees, USF, GST and VAT. Once setup a tax type is selected when configuring a Tax or Tax Source.

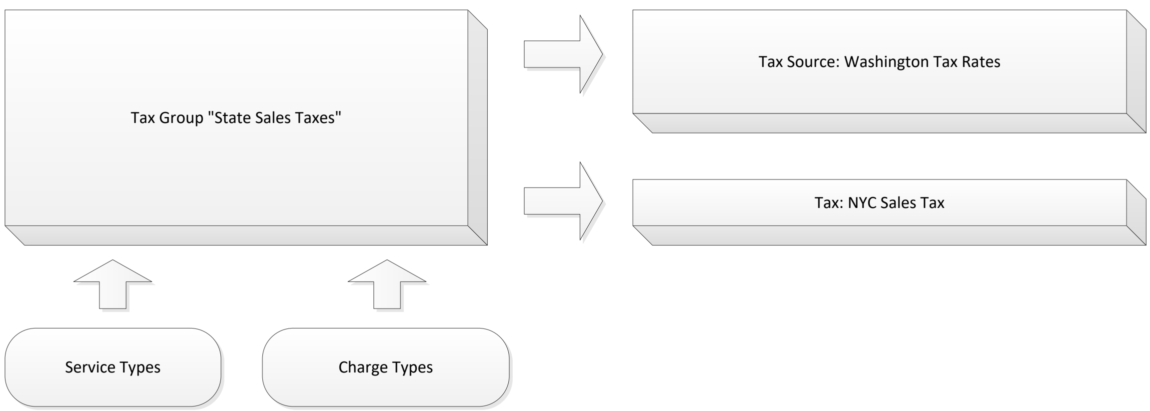
Primary purpose of tax types is grouping of related taxes within a tax group such that only best matching tax of a given tax type may be selected for tax calculation. For example if a state charges a single tax rate except for a few areas where the rate is different a tax group would typically be setup with a general tax applying the standard rate covering the entire state followed by more specific taxes targeting those areas where tax rate is different. Tax type grouping prevents both the general tax and area specific tax rates from both being assessed insuring only the single best matching rate per tax type within a tax group will be selected.

Tax Groups

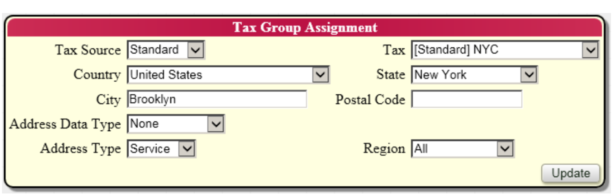
Tax groups are used to define the rate and structure of taxes applied against invoice line items during the billing process. Once a tax group has been defined it can be assigned to any number of Emerald service types and charge types to enable taxes to be assessed for these items as required.



Source	Tax Type	Description	Address	Country	State	City	Zip	Region	Address Data
State Sales Tax									
WA State Taxes	Sales Tax		Service	United States	Washington	All	All	All	WA Tax Place: *
Standard	Sales Tax	NYC	Billing	United States	New York	Bronx	All	All	
Standard	Sales Tax	NYC	Billing	United States	New York	Brooklyn	All	All	
Standard	Sales Tax	NYC	Billing	United States	New York	Manhattan	All	All	
Standard	Sales Tax	NYC	Billing	United States	New York	Queens	All	All	
Standard	Sales Tax	NYC	Billing	United States	New York	Staten Island	All	All	



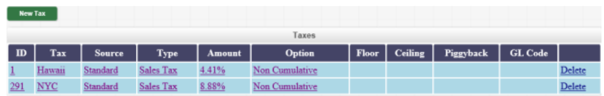
Tax groups provide a grouping of taxes and tax sources. Membership of taxes within a tax group can be made conditional based on address type, country, state, city, postal code, region and address custom data fields. When assigning multiple taxes of same tax type and more than one tax of same tax type match then the most specific match is used. Order of fields from least to most specific: State, City, Postal Code, Region and Address Data.



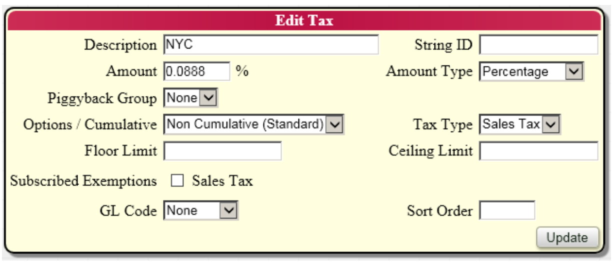
Field	Description
Tax Source	When "Standard" is selected individual taxes configured within taxes menu are able to be chosen for assignment to the tax group. Otherwise all taxes synchronized with the chosen tax source are applied to the tax group.
Tax	When tax source is "Standard" a tax is selected for assignment to this tax group
Country	When tax source is "Standard" selected tax is applicable only when the accounts country matches
State	When tax source is "Standard" selected tax is applicable only when accounts state matches
City	When tax source is "Standard" selected tax is applicable only when accounts city matches
Postal Code	When tax source is "Standard" selected tax is applicable only when accounts postal code matches

Address Data Type	When tax source is "Standard" selected tax is applicable only when selected accounts address custom data field matches Address Data configured below.
Address Data	When tax source is "Standard" and the Address Data Type field above has been configured the tax is only applicable when address data matches the address custom data field value.
Address Type	Determines which address at MBR and Service levels is to be used for the purpose of address matching of taxes.
Region	Selected tax or tax source is applicable only when the accounts region matches

Taxes



Taxes define basic tax rates to be levied against invoices. Once a tax is created it is available for assignment to tax groups which determine overall policy for taxing by service and charge types. Many tax structures are supported including single, double and piggybacked tax calculations, tax floors, ceilings and limits.



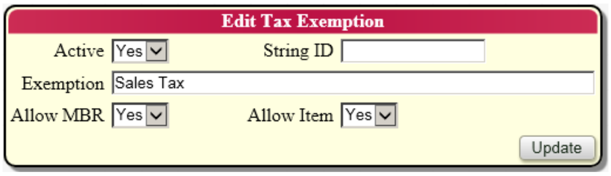
Field	Description
Description	Enter an identifying description for the Tax. Description is presented to represent this tax when assigning this tax to a tax group.
String ID	See Common fields
Cumulative	This option indicates whether the tax is to be applied individually to each charge item, or applied to the cumulative total charges for the MBR over the billing period. Choose 'Cumulative' if the tax is to be applied over the accumulated MBR billing period charges. Choose 'Non-Cumulative' if the tax is to be applied individually per taxable item. Note: This selection will affect the application of Tax Limits, as an accumulative tax will apply the tax limits to the cumulative MBR charge totals and not individually per account charge. For example, if an Accumulative tax with a tax Floor of $15.00 is applied to an MBR with 2 services charged at $10/each, Emerald will apply no tax to the first $10.00 service and only apply tax to the last $5.00 of the second tax ($20.00 MBR total, less the $15.00 floor). A non-accumulative tax with a $15.00 floor would not apply any tax to the above services, as the $10.00 charge falls below the $15.00 Floor in both cases. The 'Non-Cumulative Monthly' options apply ceiling and floor calculations on a monthly basis for recurring accounts regardless of the payment period of the services. For example using the 'Cumulative Monthly' setting with an account billed once on a yearly basis breaks up all service costs on a monthly basis, applying ceiling and floor constraints at a monthly rather than yearly level. For most simple taxes the cumulative option should be set to its default of 'Non-Cumulative'. When Price Inclusive is selected the cost of the line item being taxed is decremented from the taxable amount of that line item. For example a 10% tax on a 100.00 (tax inclusive) line item generates a tax

	line item of 9.09 changing the line items original price from 100.00 to 90.91.
Tax Type	Provide grouping of similar taxes within a tax group in a way that only one tax within the tax group of the same tax type is applied to a given item taxed. Recall that typically within a tax group all taxes matching the group's criteria (location, region, exemptions etc.) apply to each taxable item. With tax groups only one tax having the same tax type within a tax group is applied. The decision of which tax to apply is based on the tax with the most specific location matching the MBR. For example a tax having Country, State and City defined matching the MBR is more specific than a tax where only a Country and State have been defined and match. Tax types are primarily intended to allow for variations of the same tax within a geographic area. If no tax type is selected all taxes matching the location and region criteria of the tax group are applied for all taxes in the tax group having no tax type. Tax types are configured from Tax Types located in the Emerald Admin / Accounting menu.
Amount	Enter the tax rate in its direct numeric form. For example, an 8.1% tax rate is entered "8.1".
Amount Type	The type of the amount stored in the amount field. When "Percentage" the Amount field is a tax percentage of taxable items. When 'Static Amount' the amount field is a static taxable amount regardless of the cost of the taxable item.
Piggyback Group	Piggyback groups provide for "Tax on Tax" configurations. Within an invoice taxes having the same piggyback group set use "Piggyback Order" field below to control the order tax is applied to subsequent taxes. Piggyback taxes can only be applied to percentage based taxes however static taxes can contribute to tax on tax amounts. Tax floor and ceiling limits are not applicable to tax on tax portions of taxable amounts.
Piggyback Order	Sets "tax on tax" order within a piggyback group starting from lowest order to highest. For example within an invoice there are two taxes GST and VAT having same piggyback group. GST is configured order 1. VAT is configured order 2. VAT tax includes all taxes within the piggyback group before itself (order less than 2) and therefore GST amount contributes to taxable amount of VAT. If there are additional taxes with higher orders the taxable amounts of all lower orders including all prior outcomes of tax on tax calculations are applicable. If multiple taxes share the same piggyback group and piggyback order neither tax contributes to other taxes of the same order.
Subscribed Exemptions	When a tax subscribes to an exemption that tax will not be charged if one or more MBR, service type or charge type also have one or more matching exemption enabled.
Floor Limit	A Tax Floor defines what amount the item cost must reach before it is taxed. With a Floor Limit, tax will only be imposed if the item total reaches the Floor value. Tax will only be imposed on the item cost, less the Floor Limit amount.
Ceiling Limit	A Tax Ceiling defines what amount the item tax amount must reach before it can no longer be taxed. With a Ceiling Limit, tax will only be imposed up to the ceiling limit.
GL Code	GL Code for this tax.
Sort Order	See Common fields

Tax Exemptions

Exceptions to normal taxation for individual MBRs or categorically by service type or charge type are configured within this menu. To create exemptions select an available unused exemption from the list. There are a finite number of assignable exemptions.

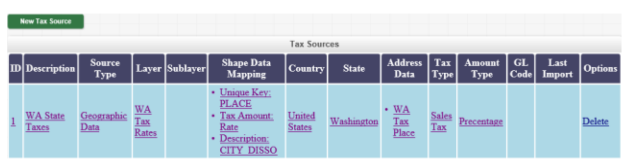
To be applicable an exemption must be assigned to one or more tax or tax source as well as assigned to MBRs by editing MBR in the Emerald client or assigned to a service type or charge type. When both an applicable tax and MBR, service type or charge type have one or more exemptions in common tax is not charged.



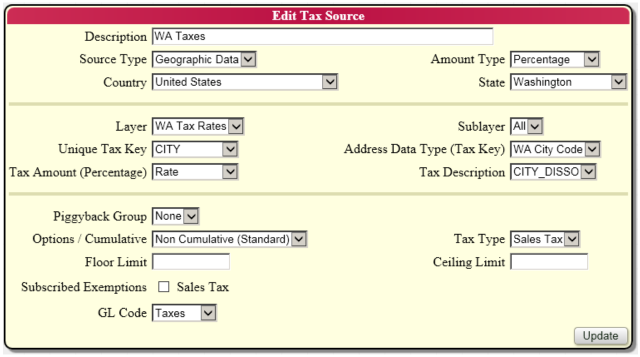
Field	Description
Active	When active the tax exemption is available for selection and the exemption is enforced. When inactivated exemption is no longer available for selection and any existing exemption assignments are not enforced.
StringID	See Common fields
Exemption	Unique description of the exemption displayed to operators when managing this exemption.
Allow MBR	When allowed exemption is made available as an option at the MBR level via MBR edit form. If disabled exemption is not selectable when editing MBRs however any pre-existing exemption assignments are maintained and still applicable unless this exemption is inactivated.
Allow Item	When allowed exemption is selectable at the service type and charge type levels allowing exemption to be applied categorically by specific service type and charge type. If disabled exemption is not selectable when editing service types and charge types however any pre-existing exemption assignments are maintained and still applicable unless this exemption is inactivated.

Tax Sources

Tax sources manage automatic import and synchronization of tax rate data from external datasets loaded via geographic layers or imported to TaxRates table. Once a tax source has been created all taxes generated as a result of synchronization from the external dataset is available for assignment to one or more tax groups.



ID	Description	Source Type	Layer	Sublayer	Shape Data Mapping	Country	State	Address Data	Tax Type	Amount Type	GL Code	Last Import	Options
1	WA State Taxes	Geographic Data	WA Tax Rates		• Unique Key: PLACE • Tax Amount: Rate • Description: CITY_DISSO	United States	Washington	• WA Tax Place	Sales Tax	Precentage			Delete



<table>
<tr><th>Field</th><th>Source</th><th>Description</th></tr>
<tr><td>Description</td><td>All</td><td>Enter an identifying description for the tax source. Description is presented to represent this tax source when assigning the source to a tax group.</td></tr>
<tr><td>Source Type</td><td>All</td><td>Selects external data source for tax rate synchronization.

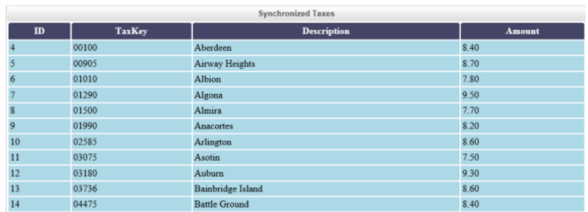
<table>
<tr><th>Source Type</th><th>Description</th></tr>
<tr><td>(Geo)graphic Data</td><td>Data will be sourced from a geographic layer loaded into emerald using the geoimport utility. If the dataset is refreshed by running geoimport to import a newer version of the same dataset then tax rate data will be automatically resynchronized by geoimport during the data import. For more information see Layers.

When layers are used for tax determination following prerequisite configuration is generally also necessary:
Enable geocoding of addresses to determine approximate latitude and longitude coordinates of each address.
Configure address layer data matching to perform geographic query of addresses coordinates assigning resulting "Unique Tax Key" to an address level custom data field.</td></tr>
<tr><td>TaxRates Table</td><td>TaxRates is a table within the Emerald database intended for external tax rate datasets to be imported into Emerald using external data import tools. For more information about format and use of this see TaxRates.</td></tr>
</table></td></tr>
<tr><td>Import Format</td><td>TaxRates</td><td>Selects a desired tax rate data file format for upload of tax rates via Import menu option of tax sources list.

Choose "Manual" when you will be uploading data to TaxRates table directly via database rather than browser file upload.</td></tr>
<tr><td>Amount Type</td><td>All</td><td>When taxes are created from external dataset this determines whether the tax rate field of that dataset is defined on a percentage or static cost basis.</td></tr>
<tr><td>Default Country</td><td>TaxRates</td><td>If configured sets a default country for purpose of restricting applicability of tax to accounts having a matching country. Default country is overridden if the CountryID field of TaxRates table is non-null.</td></tr>
<tr><td>Default State</td><td>TaxRates</td><td>If configured sets a default state for purpose of restricting applicability of tax to accounts having a matching state. Default state is overridden if the StateID field of TaxRates table is non-null.</td></tr>
<tr><td>Address Data</td><td>TaxRates</td><td>If configured then applicability of tax is limited to account addresses having selected</td></tr>
</table>

Type		Address Data Types assigned where value matches AddressData column of the TaxRates table.
Country	Geo	If selected tax source is applicable only when the accounts country matches
State	Geo	If selected tax source is applicable only when the accounts state matches
Layer	Geo	Selects the geographic layer to be used for sourcing data for tax rate synchronization
Sublayer	Geo	Sets an optional sublayer of the layer to restrict sourcing of data for tax rate synchronization.
Unique Tax Key	Geo	Field of the geographic layer selected above which uniquely and persistently across subsequent layer updates represent each tax rate.
Address Data Type (Tax Key)	Geo	Selects address custom data field where values matching "unique tax key" above are stored. This data is generally obtained by geographic query configured by address layer data matching.
Tax Amount	Geo	Field of geographic layer selected above containing the tax percentage or static tax amount of the tax rate.
Tax Description	Geo	Field of geographic layer selected above containing a description of the tax rate.
Piggyback Group	All	Piggyback groups provide for "Tax on Tax" configurations. Within a tax group taxes that have a piggy back group set use the "Piggyback Order" field to control the order multiple taxes are applied in.
Options / Cumulative	All	Applies Taxes / Cumulative setting to all tax rates synchronized by this tax source
Tax Type	All	Applies Taxes / Tax Type setting to all tax rates synchronized by this tax source
Floor Limit	All	Applies Taxes / Floor Limit setting to all tax rates synchronized by this tax source
Ceiling Limit	All	Applies Taxes / Ceiling Limit setting to all tax rates synchronized by this tax source
Subscribed Exemptions	All	Applies Taxes / Subscribed Exemptions setting to all tax rates synchronized by this tax source
GL Code	All	Applies GL Code to all tax rates synchronized by this tax source

Once a tax source is created all tax rates currently synchronized from external data source are displayed just below the "edit tax source" form when selecting a source from tax sources list. Displayed data allows for manual review of synchronized taxes to confirm successful import.



Synchronized Taxes

ID	TaxKey	Description	Amount
4	00100	Aberdeen	8.40
5	00905	Airway Heights	8.70
6	01010	Albion	7.80
7	01290	Algona	9.50
8	01500	Almira	7.70
9	01990	Anacortes	8.20
10	02585	Arlington	8.60
11	03075	Asotin	7.50
12	03180	Auburn	9.30
13	03736	Bainbridge Island	8.60
14	04475	Battle Ground	8.40

TaxRates Table

Table "TaxRates" located within the Emerald database is available for external import of tax rate information from external sources into Emerald using third party data import tools. Before importing data into TaxRates it is first necessary to create at least one Tax Source having a source type of "TaxRates Table".

Field	Type	Required	Description
TaxSourceID	Integer	Yes	Unique identifier of tax source this rate is to be applied to. TaxSourceID corresponds to 'ID' field of configured tax source displayed when viewing Emerald Admin / Accounting / Tax Sources.
ExternalRef	String	Yes	A unique reference key of external dataset to be imported which uniquely identifies the tax. For example if importing a list of taxes by postal code external ref may simply be postal code. In other contexts it may represent a unique reference code assigned by the taxing authority.

			ExternalRef should be as stable as possible when subsequently updating or reimporting future tax rate changes into this table. For example a tax representing Region A when data is imported initially should have the same ExternalRef value representing Region A in any future imports. It is important to avoid reassigning a preexisting ExternalRef value to a new unrelated tax or creating new ExternalRef values for previously imported taxes.
Description	String	No	Description is set in the Description field of the corresponding tax once synchronized which provides a user friendly name for the tax.
Tax	Money	Yes	Tax rate. For example a 7.5 percent tax is entered as 7.5
CountryID	Integer	No	If tax is to be limited to a country this represents the UN country code of the country tax is to be applicable. The codes can be determined from the 'UN ID' column when viewing Emerald Admin / Geography / Countries. If CountryID is not specified (NULL) then "Default Country" configured within the Tax Source is used. If CountryID is not set and no default country is configured then this tax will not be limited by country.
StateID	Integer	No	This restricts applicability of tax to a state or province within a country specified above. State ID is determined by 'ID' column in the states and provinces list when clicking on a country from Emerald Admin / Geography / Countries. If StateID is not specified (NULL) then "Default State" configured within the Tax Source is used. If StateID is not set and no default state is configured then this tax will not be limited by state.
City	String	No	Allows tax to be limited by matching city.
Zip	String	No	Allows tax to be limited by matching postal code.
AddressData	String	No	If the Tax Sources "Address Data Type" field is set then this tax will be limited by exact match of the corresponding Address Data field value.
AddressData2	String	No	If the Tax Sources "2nd Address Data Type" field is set then this tax will be limited by exact match of the corresponding Address Data field value.
TaxTypeID	Integer	No	If TaxTypeID is not specified (NULL) then Tax Type configured within the Tax Source is used.
StartDate	Datetime	No	Unused when importing data directly to TaxRates table.

```
Once data has been added or changed within the TaxRates table it is important
to click on the Tax Source from Emerald Admin / Accounting / Tax Sources menu
associated with changes and click update within "Edit Tax Source" form.  This
action triggers synchronization of externally imported tax rate data with
Emerald Tax configuration.
```

Billing Cycles

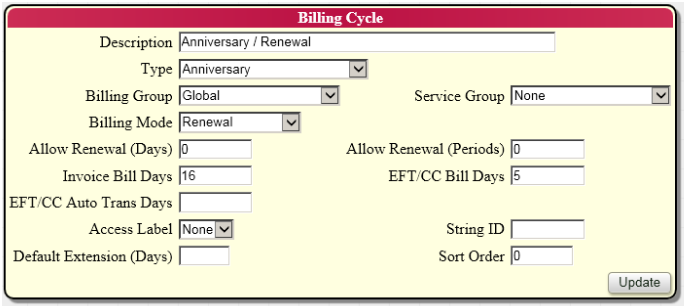
Billing cycles are assigned to MBRs to manage timing of prepaid invoice creation, automatic proration for billing day alignment and whether MBR will be recurring or non-recurring. MBR level billing cycle configuration is used in conjunction with service level pay period to define both timing of prepaid invoice generation and length of term to be invoiced.

New Billing Cycle

Billing Cycles

Description	Type	Billing Mode	Billing Day	Invoice Bill Days	EFT Bill Days	Group	Service Group	Access	
Anniversary / Renewal	Anniversary	Renewal		16	5	Global			Reset Expiry | Delete
Monthly / Renewal	Monthly	Renewal		16	5	Global			Reset Expiry | Delete
Calendar / Renewal	Calendar	Renewal		16	5	Global			Reset Expiry | Delete
Anniversary / Balance Forward	Anniversary	Balance Forward		16	5	Global			Reset Expiry | Delete
Monthly / Balance Forward	Monthly	Balance Forward		16	5	Global			Reset Expiry | Delete
Calendar / Balance Forward	Calendar	Balance Forward		16	5	Global			Reset Expiry | Delete
Non-Recurring	Anniversary	Non Recurring		16	5	Global			Delete

Billing cycles also determine overall strategy for handling nonpayment of invoices by selection of "renewal" and "balance forward" billing modes.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Enter the identifying name for the Billing Cycle. This description will be used within the ‘Billing Cycle’ selection pick lists throughout Emerald.</td></tr>
<tr><td>String ID</td><td>See Common fields</td></tr>
<tr><td>Type</td><td>Select the type of Billing Cycle being created. The Billing Cycle type determines when the Emerald will perform the billing on the account. The options are described below:
<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>Monthly</td><td>Regardless of when the account is created recurring services will be automatically prorated if necessary to align their billing day of month to the "Billing Day" configured below. If Billing Day field below is blank then the first of the month is assumed.

For example if a new MBR and service are created on the 15th of the month then the initial invoice will contain a prorate for 15th thru last day of the month and the service will subsequently be billed for each calendar month from the 1st to the last day of each month.</td></tr>
<tr><td>Anniversary</td><td>Sets the start of the billing cycle to match the day of month the MBR has been opened.

For example if a new MBR and service are created on the 15th of the month then the initial invoice will be from the 15th thru the 14th of the next month and repeat the same for all subsequent invoices. If new services are later added to the account on different days they are automatically prorated if necessary to align to the 15th of the month.</td></tr>
<tr><td>Anniversary (Period Aligned)</td><td>Similar to Anniversary except Emerald also attempts to pro-rate multi-month services so that billing month is aligned with other services in the MBR sharing the same pay period and having the highest billed thru date.

Period alignment is intended only to minimize number of invoices issued and does not itself determine when invoicing occurs. If the particular month of year invoicing occurs is important consider using "Calendar" type and configure "Billing Month" within the MBR to define starting month of the calendar year.</td></tr>
<tr><td>Calendar</td><td>Like the "Monthly" option, also sets start of the billing period to "Billing</td></tr>
</table></td></tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr>
<td></td>
<td>Day" however; this option will additionally align any pay period of the service greater than one month to a true calendar-based cycle. For example, quarterly pay period billing will be aligned with standard calendar-based quarters instead of just billing at quarterly three month intervals beginning from the service account Start Date. Calendar billing requires all pay periods within the MBR be factors of 12 (2, 3, 4, 6 and 12 months). If a services pay period is not a factor of 12 then no month level proration is performed and "Calendar" type is functionally equivalent to "Monthly" for that service.</td>
</tr>
<tr>
<td>Unaligned</td>
<td>Disables automatic proration used to align service billed thru day to MBR billing day. When selecting unaligned please carefully consider the following.

• MBRs having multiple services invoice and expire at different times during the month.
• MBR anniversary day of month for postpaid usage billing and monthly time/data limit renewal differ from period services are invoiced.
• Creation of additional invoices and associated notifications per month than would otherwise occur.
• MBRs on CC/EFT autopay may be automatically charged several times within a billing month.</td>
</tr>
</table>
</td>
</tr>
<tr>
<td>Billing Mode</td>
<td>Selects billing rules applied to the MBR.

<table>
<tr><th>Billing Mode</th><th>Description</th></tr>
<tr>
<td>Renewal</td>
<td>With this billing mode recurring services are billed automatically provided they have not expired or the "Allow renewal (days)" and "Allow renewal (periods)" have not been exceeded. Renewal billing uses the service expiration date field.

For example if a customer is prepays monthly for network access service and at some future point decides to stop prepaying for service then account is automatically expired and no new invoices are subsequently generated while the account remains in expired state.

Eventually based on Emerald Admin / Accounting / Settings configuration after a preset time has passed where account remains in this state account will automatically be closed and finally automatically inactivated generally without operator intervention assuming closure of account results in a settled account balance.</td>
</tr>
<tr>
<td>Balance Forward</td>
<td>This mode bills recurring services indefinitely regardless of the payment status of previous invoices. Balance forward billing uses the MBRs credit limit in lieu of a per service expiration date to prevent customers who have not paid for service from accessing their accounts.</td>
</tr>
<tr>
<td>Non Recurring</td>
<td>This mode disables all automatic recurring billing for the MBR. When used the customer and or operator must explicitly purchase and fully pay for the service before it is granted. In this mode the expiration field is used to determine account expiration. Additionally MBR licenses are counted against an active MBR only when there are one or more services that have not yet expired. Non-recurring billing is useful for providing pre-paid "Pay-As-You-Go" services. See "Admin / Accounting / One Time Charges" for details on enabling pre-paid purchases.</td>
</tr>
</table>
</td>
</tr>
<tr>
<td>Allow Renewal</td>
<td>In the Renewal billing mode this determines the number of days past account expiration to still allow a service to be invoiced again for its next billing cycle. By default expired accounts are not</td>
</tr>
</table>

(Days)	invoiced until the outstanding invoice has been paid. Also see Billing Mode / Renewal above.
Allow Renewal (Periods)	In the Renewal billing mode this determines the number of billing cycles (where time is a function of the accounts pay period) past account expiration to still allow a service to be invoiced again for its next billing cycle. By default expired accounts are not invoiced until the outstanding invoice has been paid. Also see Billing Mode / Renewal above.
Invoice Bill Days	This setting determines number of days in advance of service "Billed Thru" a service should be invoiced for the next billing period. For example if service billed thru is Jan 20th and Invoice Bill Days is 15 then 15 days prior on Jan 5th service becomes eligible to be invoiced in advance for the next billing period. This setting applies only to recurring services within MBRs having "Renewal" pay method where customers pay manually and are not setup for "Credit Card" or "Bank Transfer" auto pay.
EFT/CC Bill Days	This setting determines number of days in advance of service "Billed Thru" a service should be invoiced for the next billing period. For example if service billed thru is Jan 20th and EFT/CC Bill Days is 5 then 5 days prior on Jan 15th service becomes eligible to be invoiced in advance for the next billing period. This setting applies only to recurring services within auto pay MBRs having a pay method of "Credit Card" or "Bank Transfer". This setting does not apply to MBRs with a "Renewal" pay method.
EFT/CC Auto Trans Days	Controls when billable amounts of unpaid invoices for EFT/CC auto pay customers are to be billed via EFT/CC based on count of days between current date and earliest starting date of the recurring line items of the invoice. If an invoice has no recurring line items the earliest starting date of any line item of the invoice is used. This setting must be less than or equal to the EFT/CC Bill Days field. For example assume 'EFT/CC Bill Days' is 10 and 'EFT/CC Auto Trans Days' is 4. Next invoice is created 10 days before the start of that cycle. 6 Days later, (4 days before start of next cycle) the billable amount of the invoice can be automatically charged to the customers EFT/CC account.
Access Label	See Common fields
String ID	See Common fields
Sort Order	See Common fields
Billing Group	If the Billing Cycle is only to be available to MBRs of a specific Billing Group, select the appropriate group from the Billing Group selection pick list. If the 'Global' Billing Group default is accepted, the Billing Cycle will be available to all Emerald MBRs.
Service Group	In addition to Billing Groups, this billing cycle is also accessible to service groups that include "Billing Cycles".
Billing Day	The day of the month that an account should be billed. When an account is created it will pro-rate to this day. Billing day does not apply when "Type" is "Anniversary".
Start of Calendar Year	When type is "Calendar" this setting determines starting month of calendar year for yearly, quarterly and semi-annual service. If for example starting month is January yearly services are prorated as necessary such that yearly service would be invoiced from Jan 1 thru Dec 31 each year. This is a default setting applicable only when MBR level "Billing Month" field is set to Default otherwise "Billing Month" is used as start of calendar year overriding billing cycle configuration.
Default extension (Days)	Determines a new service default permanent extension overriding Accounting / Settings / Default Expire Grace Period.
Credit Expired Period	If a service has expired past grace and full payment is received at a later time enabling this setting causes entries to be automatically applied to service timeline marking the period between expired past grace and full payment as temporarily closed using selected cancel reason.

	This has the effect of crediting services for period of time service is expired past grace thru time paid. Once timeline changes have been applied the MBR is automatically reinvoiced as necessary to align invoicing history with changes to the timeline. If service is already scheduled to be closed at the time of expiration past grace no changes are applied to the timeline to credit period account is expired past grace. If service was previous scheduled to be subsequently changed or opened between the times of expire past grace and full payment these existing scheduled changes are not modified and service shall not be fully credited for period account is expired past grace. Entries can only be added to the timeline upon full payment which depending on renewal move expiration forward strategy may differ from fraction of payment normally required to move service expiration forward.

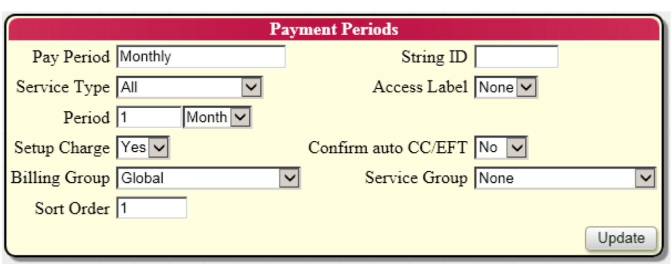
Pay Periods

Period	Service Type	Period	Setup Charge	Group	Service Group	Access	
Monthly	All	1 Month	Yes	Global			Delete
Quarterly	All	3 Month	Yes	Global			Delete
Six Months	All	6 Month	Yes	Global			Delete
Yearly	All	12 Month	Yes	Global			Delete
Weekly	All	7 Day	Yes	Global			Delete
2 Weeks	All	15 Day	Yes	Global			Delete

Pay Period defines length of the term invoiced for each recurring service. Examples of pay periods include Monthly, Quarterly, Six Months and Yearly. While rarely used pay periods can be defined in units of days rather than months. Examples include invoicing on a weekly or two week basis. Pay periods apply only to recurring accounts automatically invoiced on a subscription basis. If the MBR has a non-recurring billing cycle or a service is configured as non-recurring any pay period associated with the service is irrelevant and will remain unused for as long as the service remains non-recurring. In the case of non-recurring services only individual purchases of blocks of time/data configured by Time & Data Charges are relevant.

Within an MBR services may have different pay periods and therefore invoice at different frequencies. For example an MBR having both a monthly network access service and yearly domain service will cause an invoice to be created each month for the network access service. Once per year the invoice for network access service will also include a line item for the yearly domain service.

Pay periods can influence discounting to incentivize customers to pay for service over longer periods of time reducing administrative costs. To configure pay period discounting create a service automatic market tag matching both the desired pay period and applying the appropriate service discount for matched pay period.

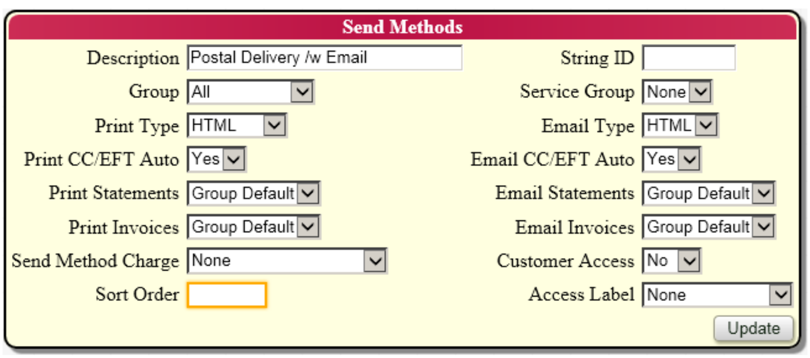


Field	Description
Pay Period	Enter the identifying name for the Pay Period. This description will be used within the 'Pay Period' selection pick lists throughout Emerald.
String ID	See Common fields

Service Type	If the Pay Period option is only to be available to Service accounts of a specific Service Type, select the appropriate type from the Service Type selection pick list. If the ‘All’ Service Type default is accepted, the Pay Period option will be available to all Emerald Services.
Access Label	See Common fields
Period	Enter the number of months or days in the Pay Period.
Setup Charge	Option to indicate if the Setup Charge associated to the Service Type applies to MBR Service accounts using this Pay Period. Choose ‘Yes’ to apply the setup charge, ‘No’ if not. For example, Service Setup Charges do not apply to those billed Quarterly.
Confirm auto CC/EFT	Determines whether automatically generated transactions for customers on CC/EFT autopay require manual confirmation by an operator before they are able to be processed. This setting is applied via MBR level default pay period.
Billing Group	If the Pay Period option is only to be available to MBRs of a specific Billing Group, select the appropriate group from the Billing Group selection pick list. If the ‘Global’ Billing Group default is accepted, the Pay Period will be available to all Emerald MBRs
Service Group	In addition to Billing Groups, this pay period is also accessible to service groups that include "Pay Periods".
Sort Order	See Common fields

Send Methods

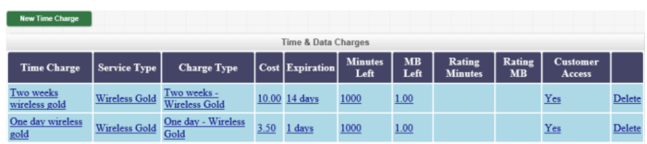
Send methods determine formatting and means by which invoices and statements are distributed to customers. Supported delivery methods include printing for postal delivery and automatic email delivery. Invoices and statements are always rendered in HTML format when using Emerald report templates. If crystal reports are used invoices and statements may also be made available for printing or Email attachment in PDF form.



Field	Description
Description	Enter an identifying description of the Send Method. This description will be used within the ‘Send Method’ selection pick lists throughout Emerald.
String ID	See Common fields
Group	If the send method option is only to be available to MBRs of a specific Billing Group, select the appropriate group from the Billing Group selection pick list. If the ‘Global’ Billing Group default is accepted, the send method will be available to all Emerald MBRs
Service Group	In addition to Billing Groups, this send method is also accessible to service groups that include "Send Methods".
Print Type	For send methods that print paper invoices and statements print type determines format printable documents are rendered to. Some print types may not be available. In the event a print type is

	unavailable the reporting engine automatically substitutes a suitable alternative.
Email Type	For email based send methods this determines the format of the email sent to the customer. Some email types may not be available. In the event an email type is unavailable reporting engine automatically substitutes a suitable alternative.
Print CC/EFT Auto	When the customers pay method is CC or EFT this controls whether invoices and statements for this customer should also be printed.
Email CC/EFT Auto	When the customers pay method is CC or EFT this controls whether invoices and statements for this customer should also be emailed.
Print Statements	Applicable only when print type is set. Overrides billing group level "Statement Batch Printing" configuration.
Email Statements	Applicable only when email type is set. Overrides billing group level "Email Statement" configuration. Yes=Send Automatically, No=Sending Disabled
Print Invoices	Applicable only when print type is set. Overrides billing group level "Invoice Batch Printing" configuration.
Email Invoices	Applicable only when email type is set. Overrides billing group level "Email Invoice" configuration. Yes=Send Automatically, No=Sending Disabled
Send Method Charge	If a charge type is selected the default amount of the selected charge type is charged to the MBR after a bill has been successfully printed for postal mailing or emailed.
Customer Access	When 'Yes' send method is available for end users to select from the customer center. Access to the customer center menu to change send methods is controlled from the Emerald Admin / Web Interface / Customer Settings menu.
Sort Order	See Common fields
Access Label	See Common fields

Time & Data Charges


New Time Charge

Time & Data Charges

Time Charge	Service Type	Charge Type	Cost	Expiration	Minutes Left	MB Left	Rating Minutes	Rating MB	Customer Access	
Two weeks wireless gold	Wireless Gold	Two weeks - Wireless Gold	10.00	14 days	1000	1.00			Yes	Delete
One day wireless gold	Wireless Gold	One day - Wireless Gold	3.50	1 days	1000	1.00			Yes	Delete

Time charges allow customers to prepay for a block of expiry, session time and data for network or service access. This feature is often used in conjunction with Internet hotspots, pre-paid card applications and refill of data limited accounts. Time charges are configured by associating a charge type defining cost of time/data allocation with a service type the time charge is intended to be used with. Once an invoice line item of the same charge type is applied to a service with a matching service type and the line item is paid in full then expiry, session time and data limits defined within the time charge are automatically credited to the service.

Time charges may be applied to accounts using any of the following methods:

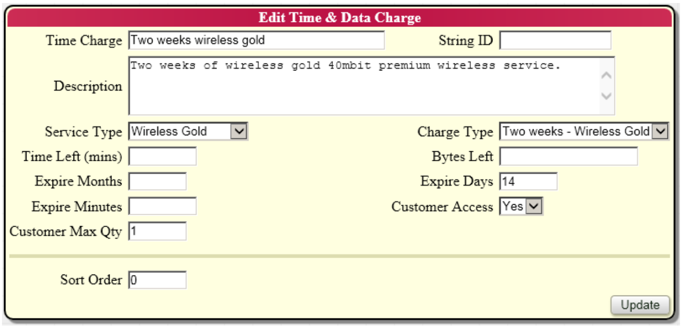
- Non-recurring customer self-signup - Requires configuration of signup option of signup server having a nonrecurring cycle type. Once service category and service type is selected within the signup option any compatible time charge is listed for selection.

- Customer account center purchase time - When the time charges customer access field is set "Yes" and the customers service type matches time charge a block of time or data may be purchased from the purchase time menu option of customer account center.

- POS invoice within Emerald client - A point of sale invoice may be created by an operator from the Point of sale menu within an MBR. Time charge can be applied only when the following conditions are met: Charge type of POS line item must match with charge type of time charge. POS line item must be applied to a service having a current service type matching the time charge. When both conditions are met the name of corresponding time charge is displayed in "Misc / Product" field of the POS line item editor. If the field is blank this means selected service and or charge type does not match any time charge therefore credit will not be issued against the service once POS line item is paid in full.

While time charges may be applied to both recurring and nonrecurring services expiry settings apply only to nonrecurring services. If a time charge is applied to a recurring service any expiry credit specified with the time charge is ignored and not transferred to the service upon payment If any service does not currently have a time or data limit set when a time charge is applied the time or data component is ignored when applying credit to service.

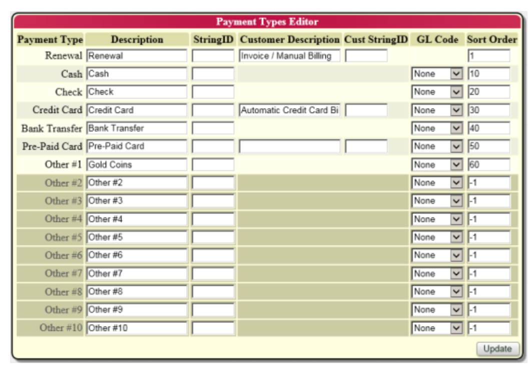
Time charges are credited to services upon full complete payment of the time charge invoice line item. Once a time charge is credited to an account this action is considered final. No compensating action is taken should a payment be subsequently changed, dishonored or invoice voided.



Field	Description
Time Charge	A short name describing the plan, this name is viewable by the customer if customer access is allowed.
String ID	Provides language support for time charge selection in the Emerald UI, while invoicing and for reporting.
Description	A detailed description of the plan. May include HTML and hyper-links. This field is visible to the customer if the customer purchased thru the Emerald customer center or signup server.
Service Type	Defines which service type is eligible to receive additional time.
Charge Type	Defines the cost and any applicable tax of the block of time being purchased.
Time Left	Online time in minutes to add to the accounts time bank when this one-time charge is paid in full. If the account does not have a time left restriction time left is not set. If the account is not expired and the existing time left value is a positive value then time left is added to the existing value. In all other cases time left is set to the time left value.
Bytes Left	Online data in bytes to add to the accounts data bank when this one-time charge is paid in full. If the account does not have a data left restriction data left is not set. If the account is not expired and the existing data left value is a positive value then bytes left is added to the existing value. In all other cases data left is set to the bytes left value.
Expire Months	Months added to accounts non-recurring expiration date once one-time charge is paid in full. If the account does not have expiration date no limit is set. If the account has expiration date in the past expiration is calculated as current time + expire months. If the account has a future expiration date expire then expire months is added to the future date. This setting has no effect on recurring services.
Expire Days	Days added to accounts non-recurring expiration date once one-time charge is paid in full. If the account does not have expiration date no limit is set. If the account has expiration date in the past expiration is calculated as current time + expire days. If the account has a future expiration date expire then expire days is added to the future date. This setting has no effect on recurring services.

Expire Minutes	Minutes added to accounts non-recurring expiration date once one-time charge is paid in full. If the account does not have expiration date no limit is set. If the account has expiration date in the past expiration is calculated as current time + expire minutes. If the account has a future expiration date expire then expire minutes is added to the future date. This setting has no effect on recurring services.
Customer Access	When "Yes" customer may purchase this one time charge from the customer account center. When "No" this item may only be purchased during signup or by an Emerald operator by creating POS invoice having a charge type matching this one time charges charge type and assigned to a service having a matching service type. The "Emerald Admin" / "Web Interface" / "Customer Settings" / "Customer Website Allow Time Purchase" option must also be enabled before customers may make unattended purchases from the customer interface.
Customer Max Qty	When customer access is enabled and the customer purchases this item from customer account center the maximum quantity user may purchase at one time is limited by this field. If not set no quantity limit is enforced
Rating Data Left	This field is similar to "Data Left" field above except data is expected to be consumed via rating engine. Using rating engine offers flexibility to conditionally consume data or consume at reduced rates based on rating criteria. For example consumption limits are not counted during on weekends or from 9 PM to 8 AM on weekdays. The "rating data left" field is separate from "data left". Both fields generally should not be used at the same time.
Rating Time Left	This field is similar to "Time Left" field above except time is expected to be consumed via rating engine. Using rating engine offers flexibility to conditionally consume time or consume at reduced rates based on rating criteria. For example consumption limits are not counted during on weekends or from 9 PM to 8 AM on weekdays. The "rating time left" field is separate from "time left". Both fields generally should not be used at the same time.
Sort Order	Used to order available purchase options within customer interface.

Payment Types



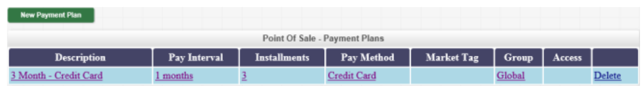
Payment Types have a dual role defining available payment methods determining MBR level renewal or CC/EFT autopay and defining payment types available when applying payment to an account. "Payment types" editor offers ability to customize labels of each payment type, hide or change order of appearance and associate GL codes for payment reporting purposes.

Payment types Other #1 thru #10 are equivalent to "Cash" type and are available for custom use. Uses are site specific however examples include processing of payments through external transaction system that does not directly integrate with Emerald. Each payment type is reported separately in payment reports and distinguishable in the MBRs payment history. If you wish to use the other #1 - 10 payment types set description field to reflect use of the payment type and adjust sort order to a positive value to make this option visible from the MBR payments menu. Finally it may be necessary to adjust allowed pay methods setting from Emerald Admin / Security / Group Rights to enable operator access to newly assigned payment type.

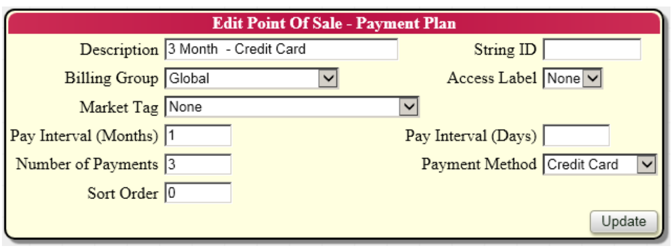
Field	Description
Payment Type	Internal description highlighting the use of the payment type.
Description	User definable description of the payment type. This description is viewable from both

	the MBR payment method selection list when editing an MBR and the payment type selection list when applying payment to an MBR.
StringID	See Common fields
Customer Description	User definable description available via the end-user customer account center
Cust StringID	Provides language support for customer center payment type selection in the Emerald UI.
GL Code	GL Code used for payment reporting
Sort Order	See Common fields

Payment Plans



When creating a "Point of Sale" invoice operators have the opportunity to assign a payment plan to spread cost of invoice over set number of payments and payment intervals. Payment plans can be fully automated where installments are handled via CC/EFT auto transactions or they can be informational only requiring manual intervention.



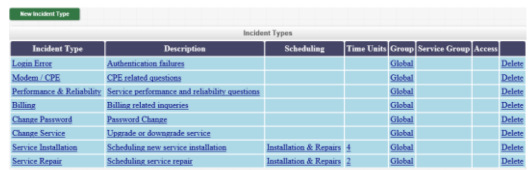
Field	Description
Description	Unique label describing payment plan. Appears in payment plan selection list within MBRs invoice menu when assigning a pay plan to an existing point of sale invoice.
String ID	See Common fields
Billing Group	See Common fields
Market Tag	If set payment plan is restricted to only those MBRs having an active MBR level market tag of the same type.
Pay Interval (Months)	Number of months between each installment payment.
Pay Interval (Days)	Number of days between each installment payment.
Number of Payments	Total number of installments
Payment Method	When credit card or bank transfer payment transactions is automatically generated on the month or day interval between installments. When Renewal payment must be applied manually. Creation of automatic transactions requires "Export CC/EFT transactions" scheduled task to be active from Emerald Admin / Scheduler / Configure Schedule.
Sort Order	See Common fields

INCIDENTS

An incident is similar to a "case" or "ticket" in other systems. Uses of Incidents include tracking customer inquiries, sales, appointment scheduling, outages and recording progress of projects. Both operators from Emerald client and customers through customer account center have the ability to create and manage incidents.

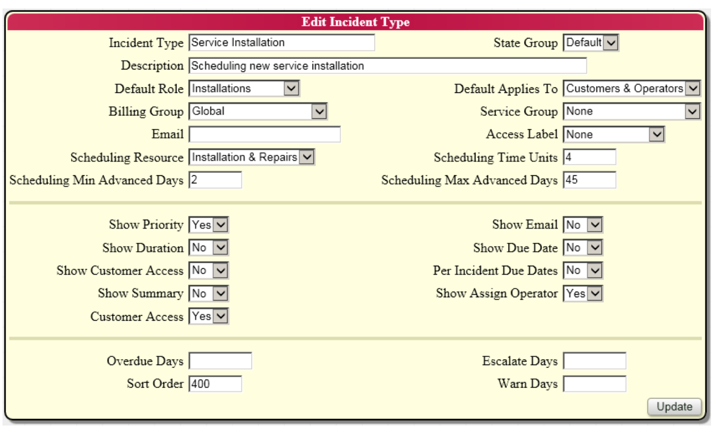
Incident Types

When creating an incident general topic or purpose of the incident is defined by incident types. Selection of an incident type controls availability of included and custom data fields, appointment scheduling resources, selectable incident states and role assignment.


New Incident Type

Incident Types

Incident Type	Description	Scheduling	Time Units	Group	Service Group	Access	
Login Error	Authentication failures			Global			Delete
Modem / CPE	CPE related questions			Global			Delete
Performance & Reliability	Service performance and reliability questions			Global			Delete
Billing	Billing related inqueries			Global			Delete
Change Password	Password Change			Global			Delete
Change Service	Upgrade or downgrade service			Global			Delete
Service Installation	Scheduling new service installation	Installation & Repairs	4	Global			Delete
Service Repair	Scheduling service repair	Installation & Repairs	2	Global			Delete

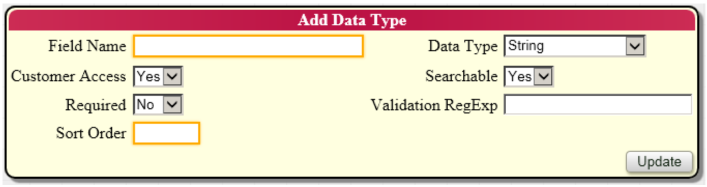


Field	Description
Incident Type	Enter a short descriptive name for the Incident Type.
State Group	Provides a listing of possible incident states applicable to this incident type.
Description	Enter a longer comment or description to clarify the Incident Type.
Default Role	For new incidents added from Emerald client or customer account center optionally configures a default role for assignment of incidents to a member of the role.
Default Applies To	When "Customers Only" default role applies to incidents created by end users from customer center only. When "Customers and Operators" default role applies to new incidents generated by operators and the customer account center.
Billing Group	See Common fields
Service Group	See Common fields
Email	This field sets a default Email address filled in automatically if "Show Email" option below is enabled and the operator creating a new incident clicks on the email field. Operator may then accept the default or set a custom address. Incidents email field is used only in conjunction with "New Incident Email" notice. This notice must be active and enabled in order for email to be sent when the incident email field is not blank.

	Generally the Incidents email field is unused. Emails related to incident assignment and actions within an incident are managed from incident assignment related notices based on operator assignment rather than incident level email field.
Access Label	When an access label is specified the operator must have at least read access to the label in order to view incidents of this type and add access to create an incident of this type. See also Common fields
Scheduling Resource	Represents resource specific availability and global calendar appointments are applied if this incident type is to be used for appointment scheduling. See Scheduling Resources
Scheduling Time Units	When incident type is used for appointment scheduling this represents the expected time required in "time units" to complete an appointment. The meaning of a "time unit" is operator defined and relative to time units allocated to time blocks within a scheduling resource.
Scheduling Min Advanced Days	When incident type is used for appointment scheduling this determines minimum amount of days advance notice is required from current time an appointment is able to be scheduled. If no advance notice is required set Min Advanced Days 0.
Scheduling Max Advanced Days	When incident type is used for appointment scheduling this determines maximum number of days from current time an appointment is able to be scheduled into the future. Maximum allowed value is 730 days. This value must be higher than value of "Scheduling Min Advanced Days" above.
Show Priority	When enabled the priority selection list is displayed. Priority is used to set the relative importance of the incident.
Show Email	When enabled the Email field used for emailing copies of the incident is displayed.
Show Duration	When enabled the Time field is available when adding incidents and actions. Total time tracked for the incident and all actions is also displayed. The time field is intended for time tracking purposes possibly to assist in the calculation of billable hours for services provided.
Show Due Date	When enabled the "Resolve By" date is displayed showing the date this incident should be marked as having been resolved.
Show Customer Access	When enabled the Customer access check box is displayed for the incident and during the creation of new actions. Customer Access allows the customer access to view incidents and actions created by an operator.
Per Incident Due Dates	When enabled the Due Date field is available when adding a new incident. The Due Date field overrides the assumed due date which is based on the "Overdue Days" field below. When an Incident is overdue the escalation procedures for overdue incidents are followed. (See Operator Roles)
Show Summary	When enabled Summary field is displayed to provide a title or short description of an incident. The Summary field is not required and if not provided or not enabled the first several words from the incident will be used in lieu of the summary field.
Show Assign Operator	When enabled an assignment field allowing the Incident to be directly assigned to an operator is presented. While manual assignment overrides automatic assignment any manual assignment must meet role requirements.
Customer Access	When enabled customers adding new incidents from the customer account center are able to select this incident type. If Customer Access is not enabled only Emerald Operators may add incidents of this type.
Overdue Days	This field determines the "resolve by" date of an incident. When an open incident is assigned to a role and has been open longer than Overdue Days the overdue escalation procedure for that role is followed.
Escalate Days	Determines number of days an open incident assigned to a role is automatically escalated following the escalation procedure for that role.
Warn Days	When set a warning is sent to the owner of the incident after an incident has been open for the number of days specified.
Sort Order	See Common fields

Custom Fields

In addition to the above field options additional custom fields can be made available with incidents by click "New Custom Field" link for an Incident Type any time after creation of the new type.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Field Name</td><td>Label defining the purpose of the custom data field.</td></tr>
<tr><td>Data Type</td><td>The type of data being stored in the custom data field.
<table>
<tr><th>Data Type</th><th>Description</th></tr>
<tr><td>Number</td><td>Field value is exclusively numeric</td></tr>
<tr><td>String</td><td>Field may contain any value unless constrained by Validation RegExp</td></tr>
<tr><td>Values from List</td><td>Field values will be selectable from a list. List of values is configured by clicking on the custom data field after it is initially added and adding one or more values.</td></tr>
<tr><td>Values from Query</td><td>Field values will be selectable from a list defined by SQL Query field below.</td></tr>
<tr><td>Configured</td><td>Custom data fields are managed from selected incident template. Incident templates are generally intended to offer add-on functionality to incidents and are not supported or documented.</td></tr>
</table></td></tr>
<tr><td>Customer Access</td><td>When set "Yes" customers are able to enter information for this custom data field from the assistance menu of the customer account center.</td></tr>
<tr><td>Access Label</td><td>See Common fields</td></tr>
<tr><td>Searchable</td><td>When set "Yes" the contents of this custom data field are searchable from the Support / Incident Search menu.</td></tr>
<tr><td>Required</td><td>When set "Yes" the operator entering a new incident is required to provide a value for this custom data field when creating or updating an incident</td></tr>
<tr><td>Validation RegExp</td><td>Perl compatible regular expression custom data field must satisfy before an incident can be created or updated. Documentation and support for creating regular expressions is not provided.</td></tr>
<tr><td>SQL Query</td><td>SQL Query used to retrieve a listing of possible values for the custom data field. The query must return a single result set containing the columns "Value" and "Description". Value contains the stored value or primary key of the selection and Description contains a textual description of the selection to the operator.</td></tr>
<tr><td>Sort Order</td><td>See Common fields</td></tr>
</table>

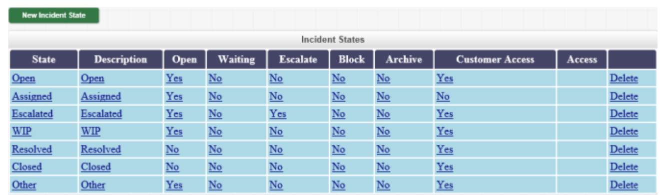
Assigned File Categories

Assigning file categories to an incident type enables files to be attached to incidents while creating or updating an incident. Removal of previously assigned file categories prevents only new assignment and has no influence on files currently attached to existing incidents.

To access attachments operators must have access to 'MBR Attachments' object group as well as access to any access labels assigned to the file category.

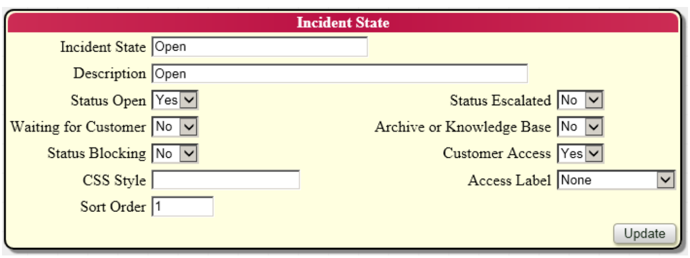
Incident States

Incident States provide for tracking status progression of incidents. Examples of incident states include open, resolved, escalated and closed. Individual states are organized into state groups. Once a state group is created it is available for assignment to one or more incident types offers some flexibility to customize those states applicable to each type of incident.



Incident States

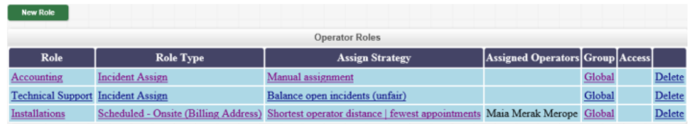
State	Description	Open	Waiting	Escalate	Block	Archive	Customer Access	Access	
Open	Open	Yes	No	No	No	No	Yes		Delete
Assigned	Assigned	Yes	No	No	No	No	No		Delete
Escalated	Escalated	Yes	No	Yes	No	No	Yes		Delete
WIP	WIP	Yes	No	No	No	No	Yes		Delete
Resolved	Resolved	No	No	No	No	No	Yes		Delete
Closed	Closed	No	No	No	No	No	Yes		Delete
Other	Other	Yes	No	No	No	No	Yes		Delete

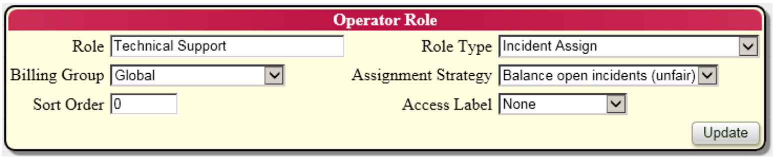


Field	Description
Incident State	Enter a short descriptive name for the Incident State.
Description	Enter a longer comment or description to clarify the Incident State.
Status Open	When enabled the Incident is considered Open and unresolved
Status Escalated	When enabled the Incident is considered Escalated and the escalation rules for the Operator role the incident is assigned are followed.
Waiting for Customer	When enabled the Incident is dependent on additional information or feedback from the customer.
Archive or Knowledge Base	When enabled the Incident is eligible to be included in a customer knowledge. Currently unused by Emerald and provided for informational purposes only.
Status Blocking	When enabled the Incident is considered important enough to block an action from occurring. An example of this would be a bug that prevents the rollout of a customer website.
Customer Access	Reserved for future use
CSS Style	Sets the table rows CSS class attribute for incidents in this state when viewing a listing of incidents or making a selection from the Status field. Setting a style can make a particular incident state stand out by changing its color or choosing a different font size or font style. Corresponding CSS class definitions are applied to stylesheets located in custom Theme Folders.
Access Label	See Common fields
Sort Order	See Common fields

Operator Roles

Assignment of responsibility for an incident is managed by operator roles. A role represents logical grouping of operators with similar responsibilities. For example all support staff may be assigned to the role of "Technical Support" and all accounting staff assigned the "Accounting" role. Whenever a new incident is assigned to a role current assignment and configuration defined for each member is examined determine which role member to assign the incident or appointment for resolution.



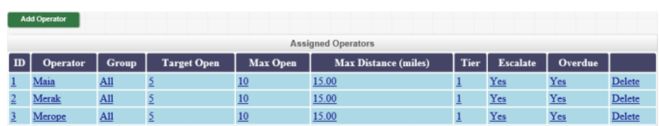


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role</td><td>Label describing the role</td></tr>
<tr><td>Role Type</td><td>Determines whether role is to be used for incident assignment or scheduling.
<table>
<tr><th>Role Type</th><th>Description</th></tr>
<tr><td>Incident Assign</td><td>This role is used for assignment of incidents to operators of this role only. Role will not be used for appointment scheduling.</td></tr>
<tr><td>Scheduled</td><td>This role is to be used for scheduled appointments such as a scheduled call for assistance or training. This role type should generally not be used for scheduling onsite appointments.</td></tr>
<tr><td>Scheduled Onsite (Service Address)</td><td>This role is used when scheduling onsite appointments to the service address associated with MBR or service linked to the incident.</td></tr>
<tr><td>Scheduled Onsite (Billing Address)</td><td>This role is used when scheduling onsite appointments to the MBRs billing address.</td></tr>
</table></td></tr>
<tr><td>Billing Group</td><td>See Common fields</td></tr>
<tr><td>Assignment Strategy</td><td>Controls method for selecting which role member the incident or appointment is to be assigned. Across all strategies the maximum open limit and tier group of each role member is respected as first priority prior to consideration of strategy.
<table>
<tr><th>Strategy</th><th>Description</th></tr>
<tr><td>Balance open incidents (unfair)</td><td>When an incident is assigned the system examines each operator’s current load of open incidents. The operator having least number of open tickets with respect to the target open count configured for the operator is assigned the incident.

This strategy is designed to favor the end customer and assumes all operators are acting collaboratively in the best interests of the customer. Operators which respond slower or otherwise leave incidents open longer will tend to be assigned relatively fewer new incidents than other operators having similar target open counts and able to respond faster.</td></tr>
<tr><td>Round-Robin distribution (fair)</td><td>Incidents are evenly distributed to operators regardless of number of open incidents they have. Round-Robin respects maximum open count configuration.</td></tr>
</table></td></tr>
</table>

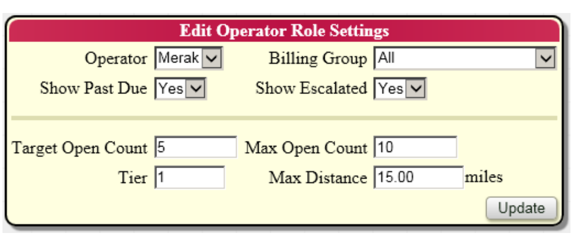
		If operators routinely reach their maximum open counts then round robin strategy can become unfair with similar properties to "balance open incidents" strategy above.
	Manual assignment	Incidents are not automatically assigned to role members. Instead role members are expected to manually claim unassigned incidents.
	Fewest appointments	Prefer role members having least number of assigned appointments within the selected time block.
	Most time remaining	Prefer role members having highest number of unassigned time units within the selected time block.
	Minimize operators	Prefers role members having already been assigned one or more appointments within the selected time block provided they have sufficient time units remaining within block to accept the assignment.
	Shortest total distance	Prefers role members having shortest straight line travel distance between operator or any of their currently assigned appointments within the same time block and the onsite customer address. Operator location is determined by site assigned to scheduling resource time block configured for the operator.
	Shortest operator distance	Prefers role members having shortest straight line distance between operator and onsite customer address. Operator location is determined by site assigned to scheduling resource time block configured for the operator.
Email	Email address of role level contact / mailing list to receive role level incident change notifications. Compatible notice types end with '(Roles)'.	
Access Label	See Common fields	
Sort Order	See Common fields	

Once a role has been configured one or more operators are assigned to the role expressing operator availability to receive incident assignments. While assignment strategy defined at the role determines how incidents are allocated to operators the target, maximums and tier groups configured per role member can also have a significant impact on frequency individual role members are assigned incidents relative to other members.


Add Operator

Assigned Operators

ID	Operator	Group	Target Open	Max Open	Max Distance (miles)	Tier	Escalate	Overdue	
1	Maia	All	5	10	15.00	1	Yes	Yes	Delete
2	Merak	All	5	10	15.00	1	Yes	Yes	Delete
3	Merope	All	5	10	15.00	1	Yes	Yes	Delete

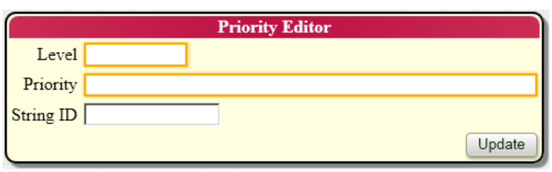


Field	Description
Operator	Emerald operator to assign to this role.
Billing Group	See Common fields
Show Past Due	If "Yes" overdue incidents assigned to the role also appear in the operators open incidents list and an overdue escalation notice is sent to the operator.

Show Escalated	If "Yes" escalated incidents assigned to the role also appear in the operators open incidents list and an escalation notice is sent to the operator.
Target Open Count	Under ideal conditions this reflects the number of open incidents this operator is expected to handle at any one time. This field is used to calculate which operator in the role is the best candidate to be assigned an incident based on operators' current distribution of open incidents.
Max Open Count	Reflects the maximum number of open incidents this operator is allowed to have.
Tier	Tiers provide for ordering of assignments to operators within a role for overflow purposes. If the "Max Open Count" for all operators in the lowest tier has been reached incidents will begin to be assigned to the tier above the lower and so on until all tiers have been exhausted. If this happens the incident is assigned to the operator least over "Max Open Count" regardless of tier. Operators in higher tiers are generally managers and operators who have a different primary job function from the role.
Max Distance	For onsite appointments reflects the maximum straight line distance between the operator and customers onsite address after which this operator is would become ineligible to be assigned the appointment. Operator location is determined by site assigned to scheduling resource time block configured for the operator.

Priorities

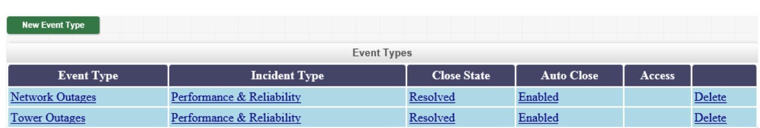
This menu provides the priority selection list available when adding or modifying an incident. It is also the source of priorities used for prioritizing late fee selection and rating rule set cost determination.



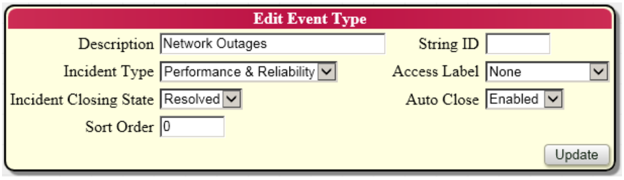
Field	Description
Level	Numeric value describing the relative priority. Lower numbers reflect a lower priority while higher numbers indicate higher priority.
Priority	Description of the priority level such as "Low", "Normal" and "High".
String ID	See Common fields

Event Types

Incidents relating to specific events affecting multiple customers such as service outages are able to be linked together and managed as a group. For example a network service outage caused by storm damage results in 150 open incidents from customer reports. Once service is restored events enable all 150 related incidents to be resolved as a group in a single operation.



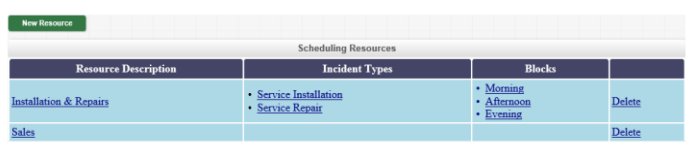
Event Types define general categories of events expected to occur. Should an event such as a 'service outage' occur an operator creates an event from Support menu of Emerald client choosing from list of available "event types" best matching the situation. Once an event is created operators are automatically made aware of the event through InfoBar notification as well as MBR and Service level alerts appearing within accounts likely to be affected.



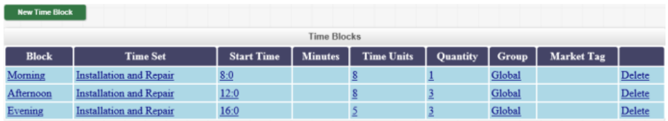
Field	Description
Description	Unique label for the event type. This field is displayed when selecting event type during creation of new events from Emerald Client / Support menu.
String ID	See Common fields
Incident Type	Incident type related to event. For example if event type is service outage then incident type selected would similarly reflect an outage, connectivity or technical questions. Incident type is used in the following ways: • When clicking on an active event from MBR or Service alert a new event linked incident entry form is provided with selected incident type set as default. • When an active event exists and a new incident is created with a matching incident type event field is automatically displayed to enable operator to associate the incident with a matching event when necessary.
Access Label	See Common fields
Incident Closing State	When an event is closed this determines final closing incident state of all event linked open incidents.
Auto Close	When "Yes" and the event is closed all associated incidents default to the incident closing state in the event closing interface. When "No" incidents assigned to the event are not defaulted. State must be selected manually for each member incident in the event closing interface.
Sort Order	See Common fields

Scheduling Resources

Scheduling resources define a global calendar incident appointments are assigned. Each resource should represent an entirely distinct non-overlapping group of responsible operators. For example scheduling resources might be defined separately for Sales vs Installation & Repair provided there is no overlap of responsible operators between these groups. For organizations where operators tend to have multiple roles it is recommended more generalized scheduling resources be created such as a single company wide resource to ensure there will be no overlap.

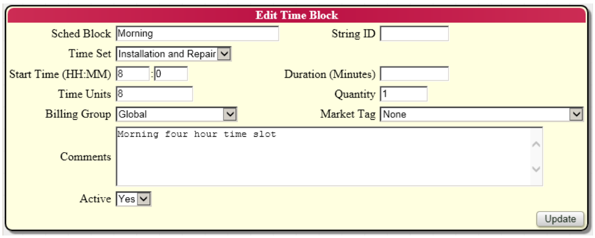


Once a scheduling resource is defined one or more blocks of time are assigned. Blocks represent time slots appointments are able to be assigned. For example blocks may be defined for morning, afternoon and evening, represent an entire business day or more granularly represent each hour of the business day.



Block	Time Set	Start Time	Minutes	Time Units	Quantity	Group	Market Tag	
Morning	Installation and Repair	8:0		8	1	Global		Delete
Afternoon	Installation and Repair	12:0		8	3	Global		Delete
Evening	Installation and Repair	16:0		5	3	Global		Delete

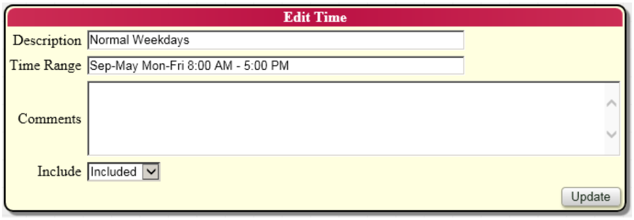
Less granular blocks offer more flexibility in timing of operators working thru assignments and scheduling optimization at the expense of communicating less specificity to customer regarding when they can expect their appointments to take place.



Field	Description
Sched Block	Unique label describing this block of time
String ID	See Common fields
Time Set	Scheduling time set defining calendar availability for this time block.
Start Time	Starting time of day of this time block. If configured start time is used when testing whether time set applies to appointment date and time block. This setting also affects chronological ordering of time blocks.
Duration	Total duration of this time block in minutes
Time Units	Number of time units available for allocation to appointments within this time block. Time units are operator defined. Each incident type used for appointment scheduling defines number of time units appointments may consume. For example assume Incident type "New Installation" is assigned 2 time units, "Onsite repair" is assigned 1 time units and this time block is configured to support 3 time units. This means within this time block the following appointments may be scheduled: • 1x - New Installation + 1x Onsite Repair • 3x - Onsite Repair
Quantity	Quantity acts as a multiplier of time units. For example if time units setting above are 3 and quantity is 2 this means a total of 6 time units are available for assignment. Generally time units is intended to reflect approximate number of time units per operator while quantity reflects expected number of concurrent operators able to respond to appointments. Quantity multiplier does not enable incident types with time units exceeding the blocks time units configured above to be scheduled. For example if an incident type "Full service installation" requires 4 time units to complete and time units for this time block is only 3 then regardless of quantity setting the appointment will not be available to be assigned within this block.
Billing Group	See Common fields
Market Tag	If configured this time block is available only to MBRs and Services where the selected market tag is active.
Comments	Additional information about this time slot
Active	When "Yes" this time block is available for new appointment assignments. When "No" new appointments cannot be assigned however existing previously assigned appointments are unaffected.

Scheduling Time Sets

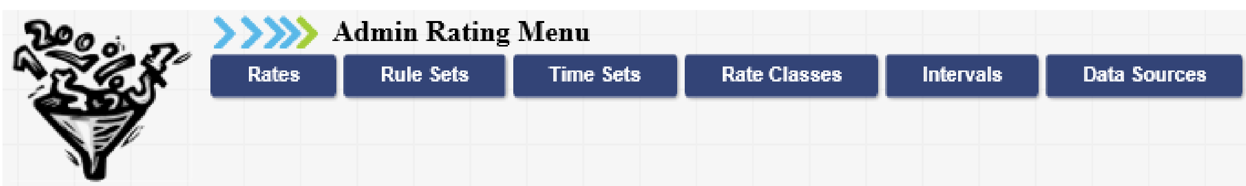
Scheduling time sets define availability for both global scheduling resource calendar and per operator calendars used to determine when appointments may be scheduled and operator availability for assignment to operators.



Field	Description
Description	Label reflecting coverage and purpose of time range
Time Range	See Common fields
Comments	Additional informational details about the time range
Include	When "Included" appointments and or assignments are permitted when time range matches appointment unless appointment matches an excluded time range. When "Excluded" appointments and or assignments are not permitted when time ranges matches appointment. Excluded takes precedence over Included. If the appointment is covered by an included and excluded time range then the appointment or assignment will not be permitted.

RATING

This menu offers management of usage-based rating of call records, network flows and third party data.



Within Emerald rating is the process of taking available usage information such as network flows or call detail records (CDR) matching this data to an account (Classification) based on defined rules and available customer information to charge the account for usage and or enforce usage limits.

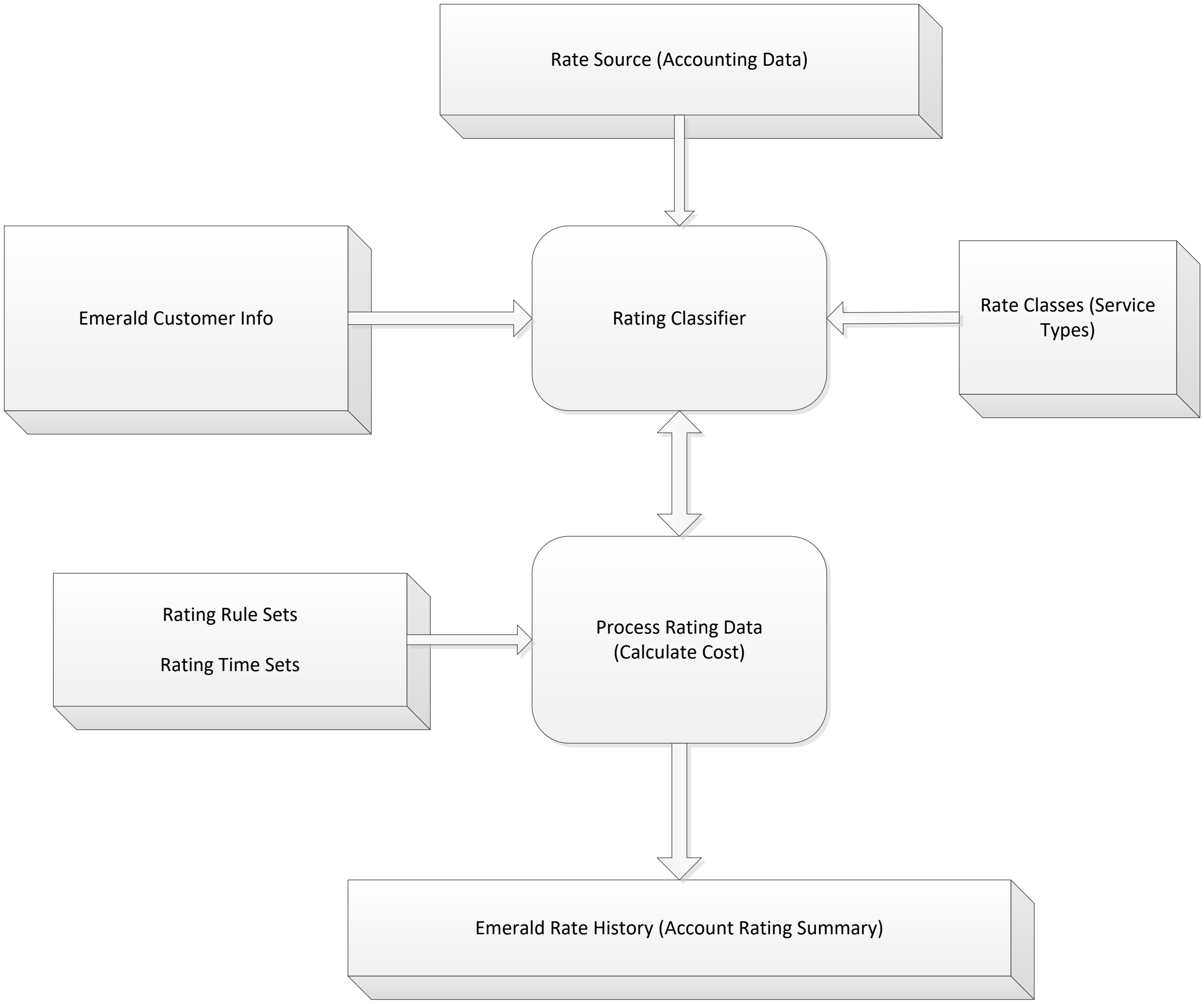
A popular example of rating is rate plans used in the cellular telephone industry where monthly plans include wording such as "300 any time minutes and unlimited night and weekend calling", "$1.00 for the first 20 minutes and .5 cents each additional minute" Emerald provides the framework to enable the configuration of both simple and complex rates and to rate data from a number of disparate sources outside of those included within Emerald.

Before we begin looking into the configuration of the Emerald rating engine it is necessary to become familiar with terms used throughout this section.

Term	Definition
Rate Source	Refers to the source of data to be rated. Examples of rating sources are "call detail records" and "network flow records"
Rating Classifier	Classifiers are rules used to associate data from a "Rate Source" with specific accounts within Emerald. An example of classification is associating the destination IP Address of a network

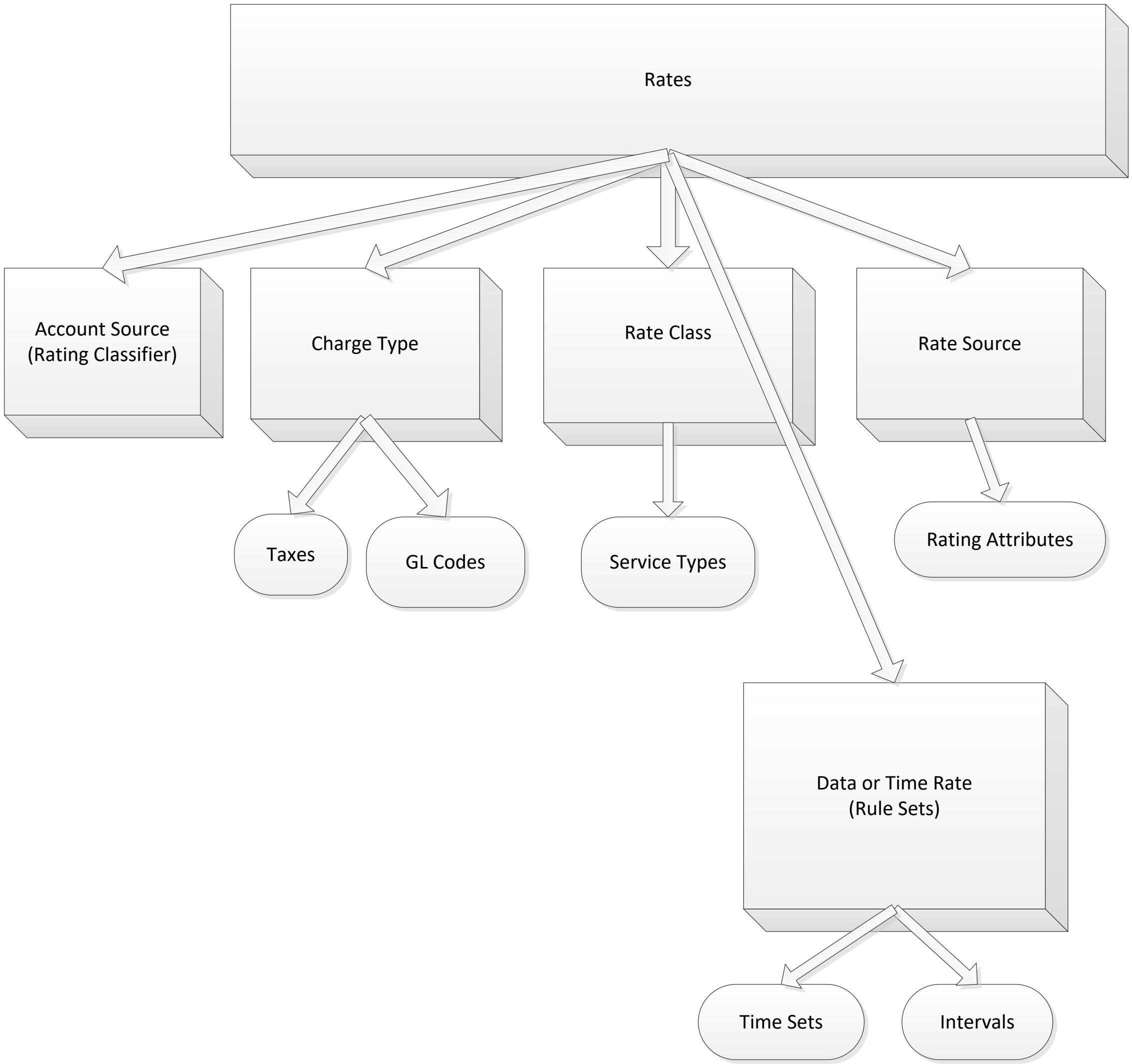
	flow record to a specific MBR/Service or associating an email address or user name to a specific MBR/Service.
Time Set	Represents a grouping of time periods such as "Nights and Weekends", "Holidays" and "Business Hours". These groupings are generally used to apply different costs based on time of day, day of week…etc.
Dimension	Refers to "what" is being rated. In most cases the rating dimension is either "Time" or "Data". Examples of a rate in the time dimension is "$1.00 per 5 hours" whereas the data dimension "$1.00 per gigabyte"
Interval	Intervals determine the units rating charges are based. Examples of Intervals are "minutes", "hours", "megabytes" and "gigabytes". Intervals are defined based on "Dimension" relative to the base units provided by a rate source such as "number of seconds" or "number of bytes"
Attribute	Represents a field from the data of a "Rate Source". Examples of fields from a call detail record include "calling number", "called number" and "call duration". Examples of fields from a network flow rate source are "Source Address", "Destination Address", "Source Bytes", "Source Port" etc.
Rule Set	In simple terms rule sets associate a cost to an interval. An example of a rule set is "10 cents per minute". Or "$1.00 per gigabyte". Rule sets provide configuration of complex rates based on the contents of attributes and or the accounts prior usage history.
Data Rate	A rule set defined in the "Data" "dimension".
Time Rate	A rule set defined in the "Time" "dimension".
Rate Class	Used for the association of Emerald "service types" with a rate. Multiple rates can be assigned to a rate class and multiple service types can be assigned to a rate. Examples of rate classes include "time limited customers", "unlimited network access" or "Priority customers".

The following diagram shows how the Emerald rating engine processes data. Data from the "Rate Source" is "Classified". Next each rate sharing the customers "Rate Class" is executed and the results summarized into Emeralds usage summary database which is later used to generate a usage charge against the customer’s account.



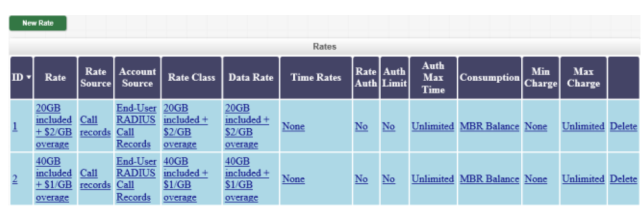
Note a single record from "Rate Source" can be rated multiple times provided that multiple rates are defined and match one of the available classifiers. This is done to support complex rate plans and settlement / reseller environments where multiple customers may be charged at different rates for the same usage record.

The following diagram is presented as a guide to show the dependencies involved when configuring a Rate. We recommend configuring items from the bottom up to in this diagram to ensure you have configured the necessary options at each level streamlining the configuration of rates.



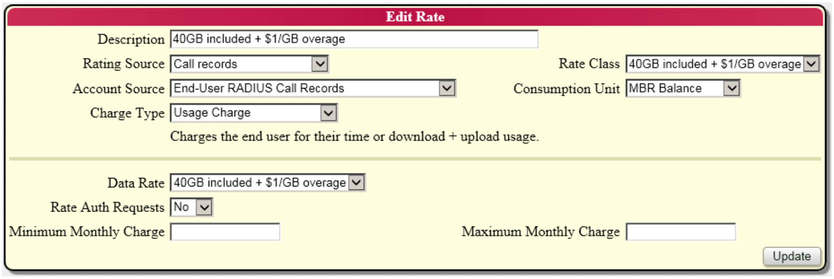
Rates

Rates join together all aspects necessary to cost usage. These include Account Source, Charge Type, Rate Class, Rate Source and Rule Sets. Before proceeding to configure Rates it is necessary to make sure Charge Types, Rate Classes and Rule Sets have first been configured.



Rates

ID	Rate	Rate Source	Account Source	Rate Class	Data Rate	Time Rates	Rate Auth	Auth Limit	Auth Max Time	Consumption	Min Charge	Max Charge	
1	20GB included + $2/GB overage	Call records	End-User RADIUS Call Records	20GB included + $2/GB overage	20GB included + $2/GB overage	None	No	No	Unlimited	MBR Balance	None	Unlimited	Delete
2	40GB included + $1/GB overage	Call records	End-User RADIUS Call Records	40GB included + $1/GB overage	40GB included + $1/GB overage	None	No	No	Unlimited	MBR Balance	None	Unlimited	Delete



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Description of the rate</td></tr>
<tr><td>Rating Source</td><td>Dataset from which to retrieve usage information for rating. Rating sources are configured from Emerald Admin / Advanced / Rate Sources.</td></tr>
<tr><td>Rate Class</td><td>Rate class of this rate must match rate class transmitted with source data or rating classifier derived rate class in order for rate to be applicable. For Call records and other included rating sources rate class is determined by the rate class associated with account service type.

Rate classes are configured from Emerald Admin / Rating / Rate Classes.</td></tr>
<tr><td>Account Source</td><td>Represents an available "Rating Classifier" for the selected rating source. See Admin / Advanced / Rate Classifiers. A helpful description of each account source is displayed once selected.</td></tr>
<tr><td>Consumption Unit</td><td>Once usage cost has been determined this setting determines both unit cost is measured and how cost is debited. Generally most rates will select MBR Balance as consumption unit.

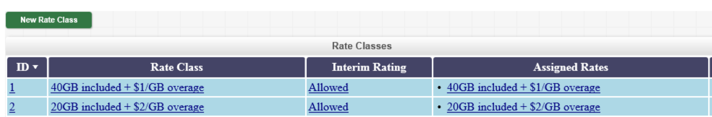
<table>
<tr><th>Consumption Unit</th><th>Description</th></tr>
<tr><td>MBR Balance</td><td>This is the recommended default consumption unit. When selected costed usage is in units of currency affecting accounts real-time balance. Once the usage billing month is completed a charge adjustment is generated to bill the customer for usage.</td></tr>
<tr><td>Summary Only</td><td>This setting tracks consumption for reporting and informational basis but does not affect account balance or generate charge adjustments for usage rollup.</td></tr>
<tr><td>Service Data Left</td><td>When selected usage is costed in terms of "data" and rating data left field at the service level is debited based on the rated data cost. The services "rating data left" field is a separate field from the standard "data left" field.

This consumption unit would typically be used if customers are given renewable monthly data allocations where consumption is conditionally not counted or counted at a different rate based on calendar or time of day.</td></tr>
<tr><td>Service Time Left</td><td>When selected usage is costed in terms of "time" and rating time left field at the service level is debited based on the rated time cost. The services "rating time left" field is a separate field from the standard "data time" field.

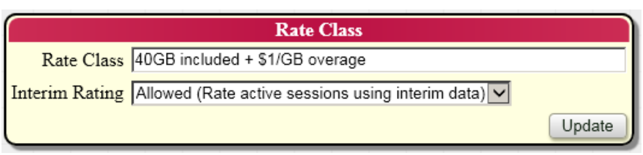
This consumption unit would typically be used if customers are given renewable monthly session duration allocations where consumption is conditionally not counted or counted at a different rate based on calendar or time of day.</td></tr>
</table></td></tr>
<tr><td>Charge Type</td><td>Represents the Emerald charge type used when rolling up service usage into a usage charge adjustment.</td></tr>
<tr><td>Data Rate</td><td>Rating Rule used to calculate usage fees based exclusively the "Data" "Dimension"</td></tr>
</table>

	regardless of time.
Rate Auth Requests	When enabled and when rating is enabled in the RadiusNT/X administrator authentication requests are rated to enforce configured usage limits and or calculate a limited session duration based on the accounts available balance.
Auth Session Limiting	When Rate Auth Requests is enabled this controls whether a session limit should be imposed based on the accounts available balance. Note that even when session limiting is disabled other forms of session restrictions configured in the Rating Rule still apply.
Auth Max Session Time (Seconds)	Used to enforce a maximum session duration after which the user must re-authenticate to regain network access.
Minimum Monthly Charge	If any network usage is recorded for the users monthly cycle this defines the minimum amount to be charged to the account. Note that if there is no network usage during the users monthly billing cycle a minimum charge is not assessed.
Maximum Monthly Charge	Defines the maximum possible amount that can be charged over the users monthly billing cycle regardless of what costs are defined.
Time Rates	Set of Rating Rules used to calculate time or data usage fees based on time period covered by usage being costed. When multiple time rates are defined then all relevant time rates are used automatically when rating data. If time rates overlap the highest priority followed by the most specific time specification is used for that period. If data consumption rates are being defined to vary conditionally based on time of day or calendar it is recommended that Interim RADIUS accounting be enabled across all access servers and within the Rate Class to enable accurate calculations of time dependent data rates. Without interim data the rating system is limited to calculations assuming constant rate of consumption across the session's timespan.

Rate Classes



Rate class is used to associate one or more Service Types to one or more Rates. Typically for each rate a rate class with the same description of the rate will be defined. Once a rate class is configured it is available for selection from any Service Type or Rate.

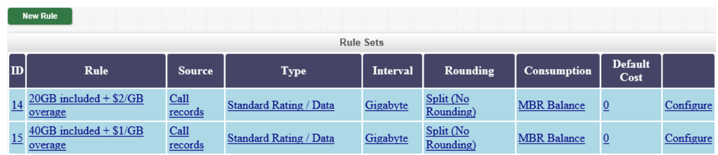


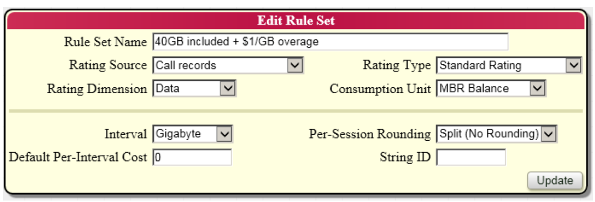
Field	Description
Rate Class	Unique label describing rate class. Displayed when selecting rate class when adding or changing a service type or rate.
Interim Rating	For rates having a rating source of "Call records" this controls whether costing is based on RADIUS stop or RADIUS interim data when available. When "Allowed" time set dependent data rates are allowed to be costed more accurately based on more granular information of recent data consumption provided from interim accounting data. Interim rating treats each portion of the session reported via RADIUS interim update as a unique session for purposes of rating. Interim rating must not be used with any rating rule sets that levy per-session fees or where per-session rounding is set to anything other than split. Doing this will cause per-session fees and per-session rounding to be performed on receipt of each RADIUS interim update.

	Disallowing Interim rating means only stop records trigger usage rating. It is recommended interim rating be disallowed unless otherwise necessary for time dependent pricing of data consumption.

Rule Sets

In simple terms rule sets associate a cost to an interval. An example of a rule set is "10 cents per minute" or "$1.00 per gigabyte". Rule sets provide configuration of complex rates based on the contents of attributes and or the accounts prior usage history.





Field	Description
Rule Set Name	Descriptive text illustrating the purpose of the rule set
Rating Source	The rate source this rule set is applied to.
Rating Dimension	Sets the "Dimension" the rule set is applied to. "Time" or "Data"
Rating Type	This controls the advanced configuration interface used when clicking the ‘Configure’ link for a rule set after choosing Admin / Rating / Rule Sets. Normally this is ‘Standard Rating’. Other interfaces may be available in the future for application specific advanced configuration of rating rules.
String ID	Provides language support for the rule set name when rendering invoices.
Interval	The "Interval" this rule set is based on.
Per-Session Rounding	Controls per record rounding cost based on Interval and Per-Interval cost.
Default Per-Interval Cost	The default cost per interval, the default cost can be overridden by configuring an advanced rating rule.

"Standard Rating" advanced configuration

Advanced configuration allows rating and authentication decisions to be made based on the contents of "Attributes" in the "Rating Source". Example below uses the Standard Rating interface.

New Standard Rule

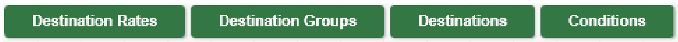
Standard Rating Configuration - 10 cents per hour

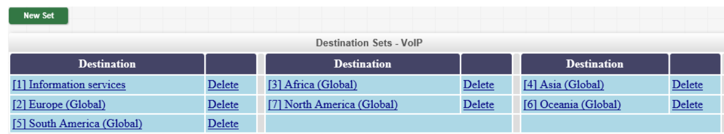
Priority	Attribute	Change Type	Match Type	Data	Attribute Description
Default	10 hour discount Cost: 0.09 Per Hour				
	TotalTime	Dynamic	Greater Than	36000	Duration in seconds across all sessions within the billing month
Default	IEA prefix lockout Default Cost / Upload Only				
	AuthReject	Static	Upload Attributes	1	If uploaded during an authentication rating request the request is rejected
	AuthRejectMsg	Static	Upload Attributes	Your telephone prefix is currently locked out	If AuthReject is uploaded during an authentication rating request with a value of Reject (1) this attribute contains an optional reject reason sent for informational purposes
	CallingStationID	Static	Begins With	509444	Phone number, MAC or other identifying network source address of the user
Default	This is a very expensive rule Cost: 2 Per Hour				
	CallingStationID	Static	Begins With	509	Phone number, MAC or other identifying network source address of the user
Default	This is an extraordinarily expensive rule (more specific than very expensive) Cost: 3 Per Hour				
	CallingStationID	Static	Exact Match	5093281111	Phone number, MAC or other identifying network source address of the user

Field	Example
Change Type	The first rule "10 hour discount" provides a small discount after the accounts total session duration has exceeded 10 hours. Note the "Change Type" column for this rule is set to dynamic. "Dynamic" attributes are constantly evaluated throughout the "Dimension" being rated while data in other dimensions are proportionally scaled and averaged in relation to the rated "Dimension". For example let's assume the session being rated has duration of 2 hours and the user's total monthly usage to 9 hours. The first hour of usage is rated at the normal fee of 10 cents per hour. However the second hour of the same session is rated at 9 cents per hour since the 10 hour discount condition has now been met.
Priority	With complex rating rules explicit and implicit priority becomes very important. Let's examine the last two rules defined here - the very expensive rule for 2/HR applies when callers phone number begins with "509" however the extraordinarily expensive rule for 3/HR applies when the caller's phone number is "5093281111" Only one rule can apply at any instant throughout the "Dimension" being rated – so what happens when the conditions of more than one rule matches? The highest priority followed by the most specific rule is chosen. The priority field provides for explicit ordering of rules however it is not always necessary or desirable to order rules explicitly such as for the example in this image – a number of factors are combined to determine what the "most specific" rule is. First the number of parameters matched is considered; second the match type combined with relevant information from the Data field. These factors are combined to determine which is the most specific. In the example in this image the rule providing an exact match for "5093281111" is more specific than the rule matching "Begins with 509" since both the type is exact match and the number of characters matched is greater.
Upload Attributes	Upload attributes are special match types, which are not actually used to match a condition and do not have any effect on the calculation of implicit priority. Instead they provide additional output to the rating engine beyond the calculation of cost when they match. Typically upload attributes are used with RADIUS authentication to enforce session limitations thru the rating engine. In the case of the example in this image "IEA prefix lockout" if the callers telephone number "begins with 509444" their RADIUS authentication request is rejected with a reply-message attribute of "Your telephone prefix is currently locked out". You could also configure restrictions for monthly data or time usage. For RADIUS authentication restrictions to be enforced the "Enforce cost-based session limits" option in the Advanced section of the RadiusNT/X admin must be enabled. Upload attributes are also used in the design of rating "Classifiers".

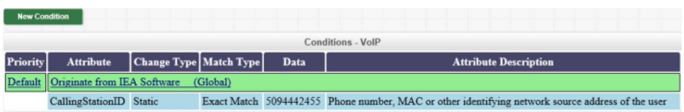
"Voice Destination Rating" advanced configuration

This rating type is used to perform rating of voice calls based on the destination number dialed. There are three main components for voice destination rating: "Destination Sets", "Destination Groups" and "Conditions".





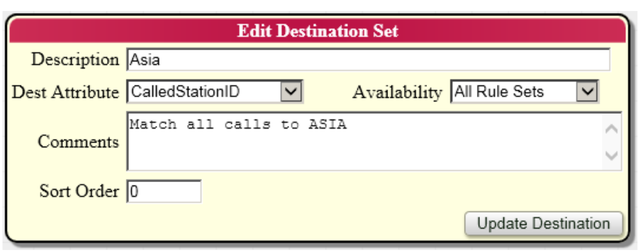
Destination sets provide a grouping of related phone numbers, destination prefix or suffix matching. An example of a destination could be an area such as a state, country or continent. Destinations may also be used to group class of services for example directory assistance and toll free numbers. Each destination set can be merged with like-minded destination sets by way of destination groups. As an example a destination group may be labeled after a country containing many destination sets covering specific geographic areas within that country.



Conditions provide matching rules or authorization changes for destination sets. Examples of conditions used for matching are application of special pricing based on calling number, port or device type. An example of an authorization condition would be to reject RADIUS voice call authorization requests where the dialed number matches a particular destination set or inject any RADIUS reply attributes into the authorization response.

DESTINATION SETS

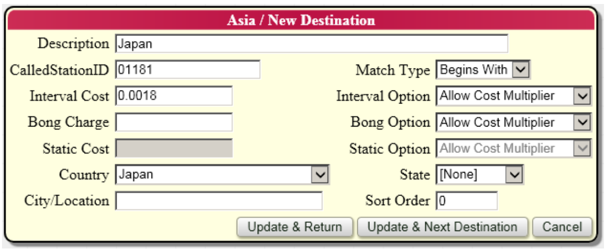
Destinations represent logical grouping of rates. Once a destination has been created individual rates can be applied manually or preexisting CSV formatted rate list imported. To use a fully configured destination set for rating a destination rate must be created.



Field	Description
Description	Text uniquely describing the destination set
Dest Attribute	Rating attribute used to match the destination number or address. In most cases the correct attribute will be selected automatically for you. This may be changed if you need to match different criteria such as phone number stored in the User-Name field or the calling rather than called number.
Availability	Controls the scope of availability of this destination set throughout the system. When set "All Rule Sets" all Rating rule sets having the voice destination rating type have access to this destination set. If the destination set is intended to be specific to a single rule set setting availability to the specific rule set will prevent it from being visible to other rating rule sets.

Comments	Descriptive text describing the purpose of the destination set and any important notes operators may need to be aware of.
Sort Order	Enter a numeric value to indicate the display order of this destination set entry. The sort order is used to sort the entries from lowest to highest numerical order.

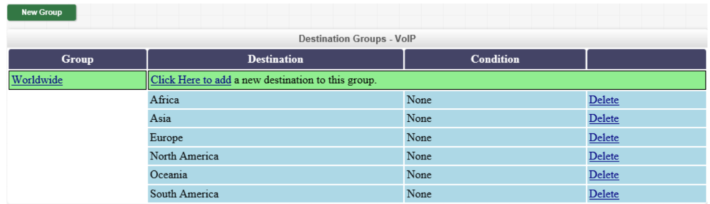
After defining the destination set multiple destinations can then be added to the set. A destination is a specific number or prefix/suffix with an associated cost. (For example dialing 5551212 costs $.25 per call)

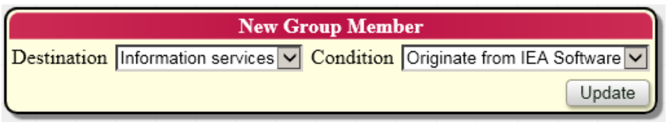


Field	Description
Description	Text uniquely describing the destination number.
NASPortDNIS	This field may be different depending on the selected "Dest Attribute" defined in the destination set above. This field always contains the number, address or prefix/suffix to be matched.
Match Type	Determines the method of matching the Dest Attribute (NASPortDNIS) field. Available options are "Exact Match", "Begins With" and "Ends With". Note that exact match has higher match precedence than begins with or ends with regardless of the number of digits matched.
Interval Cost	Sets per-interval pricing should this destination be matched. The interval is based on the interval of the rule set. Note for destination sets with Global Availability it is recommended all voice rating rule sets share a common interval to prevent confusion with pricing structures.
Interval Option	Controls whether cost multipliers defined at the "Destination Rate" level can effect this destinations pricing.
Bong Charge	Defines a static price charged to initiate the call/session in addition to any per-interval pricing.
Bong Option	Controls whether cost multipliers defined at the "Destination Rate" level can effect this destinations pricing.
Static Cost	Sets the final cost of the entire call/session at a fixed flat rate. When static cost is set Bong Charge and Interval Cost are not used for cost calculations.
Static Option	Controls whether cost multipliers defined at the "Destination Rate" level can effect this destinations pricing.
Country	Optional informational field used to report the country the Destination is associated
State	Optional informational field used to report the state the Destination is associated
City/Location	Optional information field used to report the city or location the Destination is associated
Sort Order	Enter a numeric value to indicate the display order of this destination entry. The sort order is used to sort the entries from lowest to highest numerical order.

DESTINATION GROUPS

Destination groups define a grouping of destination sets enabling all grouped destination sets to apply to a destination rate as a single unit. In the example below "Worldwide" destination group consists of destination set for each continent. Use of destination groups is optional.

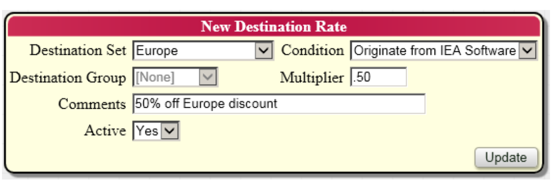




Field	Description
Destination	Destination set to add or update the Destination Group
Condition	Optional condition associated with destination group

DESTINATION RATES

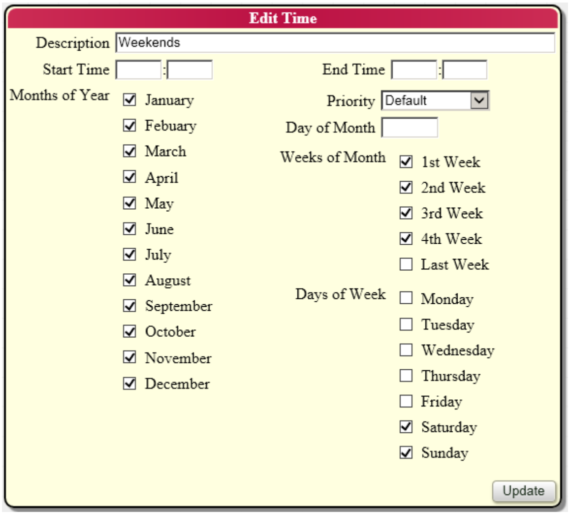
Destination rates controls which destination sets and destination groups are to be used in the rating process with an option to apply a cost multiplier based on pricing at destination level of each destination set.

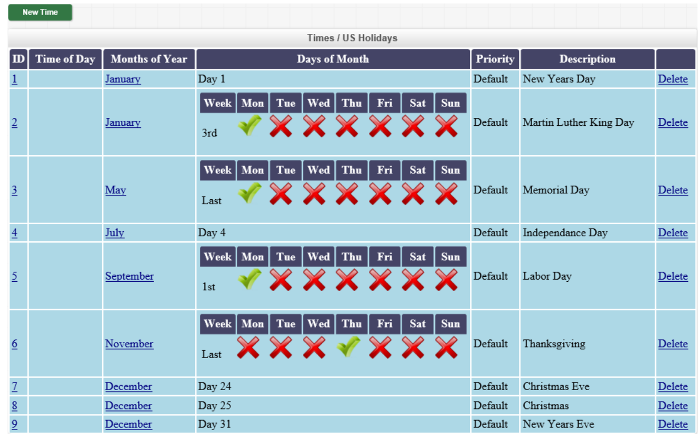


Field	Description
Destination Set	Destination set to include in the rating rule set
Condition	Condition applicable to selected destination set
Destination Group	Destination group to include in the rating rule set
Multiplier	Optional cost multiplier on each destinations price that allows a cost multiplier to be used.
Comments	Informational message describing the destination rate
Active	When Active the destination rate is included with the rating engines active rule set. When inactive the destination rate is not processed by the rating engine.

Time Sets

Time sets represent groups of time periods such as "Nights and Weekends", "Holidays" and "Business Hours". These groupings are generally used to apply different costs based on time of day and calendar.

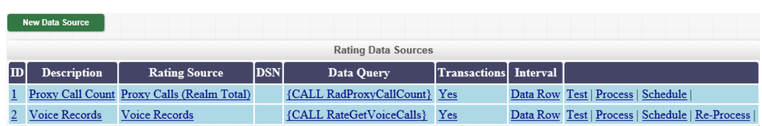




ID	Time of Day	Months of Year	Days of Month	Priority	Description	
1		January	Day 1	Default	New Years Day	Delete
2		January	Week Mon Tue Wed Thu Fri Sat Sun 3rd	Default	Martin Luther King Day	Delete
3		May	Week Mon Tue Wed Thu Fri Sat Sun Last	Default	Memorial Day	Delete
4		July	Day 4	Default	Independance Day	Delete
5		September	Week Mon Tue Wed Thu Fri Sat Sun 1st	Default	Labor Day	Delete
6		November	Week Mon Tue Wed Thu Fri Sat Sun Last	Default	Thanksgiving	Delete
7		December	Day 24	Default	Christmas Eve	Delete
8		December	Day 25	Default	Christmas	Delete
9		December	Day 31	Default	New Years Eve	Delete

Field	Description
Description	Description of the configured time. For example "New Year's Day", "Nights", "Weekends"
Start Time	If the time is based on time-of-day the start time represents the starting hour and minute the time is to apply.
End Time	If the time is based on time-of-day the end time represents the ending hour and minute the time is to apply. Note if the Ending time is less than the Starting time the period wraps thru the next days ending date.
Months of Year	Months out of the year that applies to this time.
Weeks of Month	Week numbers that apply to this time. Note that the Last week represents the last occurrence within the month.
Days of Week	Days of the week that applies to this time.
Priority	Priority is relative to all time sets applied to a rate. The most specific time having the same priority is used. Specificity is based on both yearly day coverage and daily time coverage of the individual time items within a time set.
Day of Month	If set the time interval applies to the configured day of month only. If not set "Weeks of Month" and "Days of Week" must be configured.

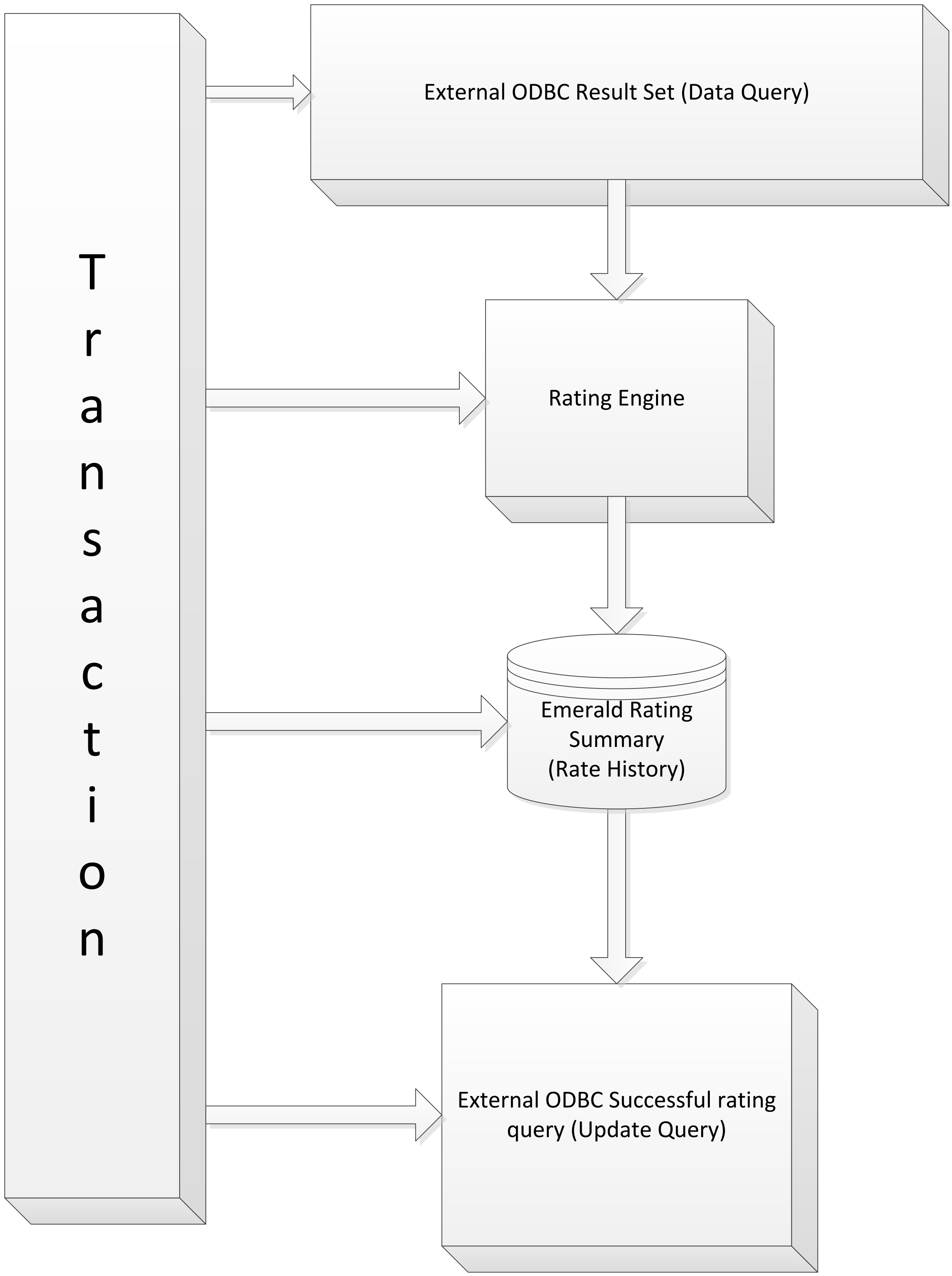
Rating Data Sources

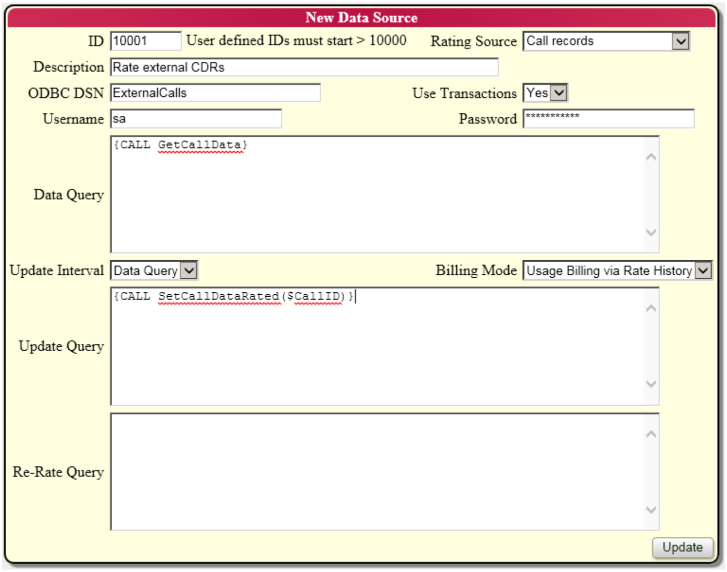


ID	Description	Rating Source	DSN	Data Query	Transactions	Interval	
1	Proxy Call Count	Proxy Calls (Realm Total)		{CALL RadProxyCallCount}	Yes	Data Row	Test | Process | Schedule |
2	Voice Records	Voice Records		{CALL RateGetVoiceCalls}	Yes	Data Row	Test | Process | Schedule | Re-Process |

Data sources provide a method of rating many forms of data contained both externally and within the Emerald database. Possibilities include external call detail records, web server access logs, firewall logs and orders. All data must be available via an ODBC datasource and returned in a single ODBC result set. On a per-record or per-query an update query can be executed to mark in the external database the record(s) having been successfully rated. When executing the query all field names available in the ODBC result set are available to be sent back for reference purposes in the update query.

Following diagram shows the process of rating external data.


T r a n s a c t i o n
External ODBC Result Set (Data Query)
Rating Engine
Emerald Rating Summary (Rate History)
External ODBC Successful rating query (Update Query)



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>ID</td><td>Internal Data Source ID which uniquely identifies this data source. When selecting a new ID you must choose a number greater than 10,000 all numbers below 10,000 are reserved for future use by IEA Software.</td></tr>
<tr><td>Rating Source</td><td>Rate source containing a listing of available attributes and a description of their use and data types within this data source. Rating Sources can be configured from the Admin / Advanced / Rate Sources menu – however this configuration is beyond the scope of this document and support services.</td></tr>
<tr><td>Description</td><td>Informational field used to describe this data source and intended use.</td></tr>
<tr><td>ODBC DSN</td><td>An optional ODBC system data source, if this field is left blank the Emerald database is used.</td></tr>
<tr><td>Use Transactions</td><td>This should always be enabled except for cases where the external ODBC data source does not support transactions. Transactions ensure consistency between rating operations and update query and protect against loss of revenue or double charging in the event of database failure.</td></tr>
<tr><td>Username</td><td>If an external ODBC DSN is defined this sets the username parameter (UID)</td></tr>
<tr><td>Password</td><td>If an external ODBC DSN is defined this sets the password parameter (PWD)</td></tr>
<tr><td>Data Query</td><td>Query used to retrieve an ODBC row set of available fields. Field names should contain alphanumeric characters only. The following internal field names hold special meaning to the rating engine and must be used as intended or avoided. Required fields do not necessarily need to be sent if a rating classifier is being used to provide the necessary information.
<table>
<tr><th>Field Name</th><th>Required</th><th>Description</th></tr>
<tr><td>RateClassID</td><td>Yes</td><td>"Rate Class" identifier specifying which rate(s) apply to the data being rated. See Admin / Rating / Rate Classes.</td></tr>
<tr><td>AccountID</td><td>Yes</td><td>Emerald service AccountID responsible for generating usage but not necessarily the account charged for usage. See CustomerID below.</td></tr>
<tr><td>BillDay</td><td>Yes</td><td>Controls the monthly period of which summary records apply. This is derived from the MasterAccounts table BillDay column for Anniversary billing cycles and BillingCycles BillDay column otherwise. If no BillDay is available the default value of 1 should be used.</td></tr>
<tr><td>Data</td><td>For Data Rate</td><td>Value of the "Data" "Dimension" this usually refers to the number of bytes, units, etc. being rated.</td></tr>
<tr><td>AmountLeft</td><td>No</td><td>Reserved, Not used</td></tr>
<tr><td>AuthReject</td><td>No</td><td>Reserved, Not used</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>AuthRejectMsg</td><td>No</td><td>Reserved, Not used</td></tr>
<tr><td>CustomerID</td><td>No</td><td>This must only be defined if you need to charge an MBR that is different from the MBR of the AccountID field above.</td></tr>
<tr><td>StartDate</td><td rowspan="3">Start + Stop OR Start/Stop + Duration for Time Rate.</td><td>Session starting date used when rating in the "Time" "Dimension" (Must return as an ODBC SQL_TIME or SQL_DATATIME type)</td></tr>
<tr><td>StopDate</td><td>Session ending date used when rating in the "Time" "Dimension" (Must return as an ODBC SQL_TIME or SQL_DATATIME type)</td></tr>
<tr><td>Duration</td><td>Session duration used when rating in the "Time" "Dimension" note that Duration should only be defined if StartDate or EndDate is not available. If both Start and End date are available Duration is ignored.</td></tr>
<tr><td>SessionTime</td><td>MUST NOT set</td><td>Internal dynamic variables, Reserved.</td></tr>
<tr><td>SessionData</td><td>MUST NOT set</td><td>Internal dynamic variables, Reserved.</td></tr>
<tr><td>SessionMaxTime</td><td>MUST NOT set</td><td>Internal variables, Reserved.</td></tr>
<tr><td>SessionMaxData</td><td>MUST NOT set</td><td>Internal variables, Reserved.</td></tr>
<tr><td>Cost</td><td>MUST NOT set</td><td>Internal variables, Reserved.</td></tr>
<tr><td>InitialCost</td><td>MUST NOT set</td><td>Internal variables, Reserved.</td></tr>
<tr><td>StaticCost</td><td>MUST NOT set</td><td>Internal variables, Reserved.</td></tr>
<tr><td>TotalTime</td><td>MUST NOT set</td><td>Internal dynamic variables, Reserved.</td></tr>
<tr><td>TotalData</td><td>MUST NOT set</td><td>Internal dynamic variables, Reserved.</td></tr>
<tr><td>TotalCount</td><td>MUST NOT set</td><td>Internal dynamic variables, Reserved.</td></tr>
</table>
</td></tr>
<tr><td>Update Interval</td><td>Controls how often "Update Query" is executed. The two choices available are "Data Query" which means once per execution of the "Data Query" and "Data Row" which means once for each row returned by "Data Query".</td></tr>
<tr><td>Billing Mode</td><td>Billing mode determines how usage fees are applied to accounts.
<table>
<tr><th>Mode</th><th>Description</th></tr>
<tr><td>Usage Billing via Rate History</td><td>Indicates usage charges will be applied based on tracked rate history data associated with rated usage.</td></tr>
<tr><td>Rate Only / No Billing</td><td>Indicates aggregate monthly usage is not tracked via rate history and charge adjustments for usage will not be automatically generated. This setting is typically used when there is an alternate method of tracking and billing usage separate from rate history.</td></tr>
</table>
</td></tr>
<tr><td>Update Query</td><td>Used to mark external data as having been rated in the external database. All field names returned in the rowset from "Data Query" in addition to the following table are available as ‘variables’.
<table>
<tr><th>Variable</th><th>Description</th></tr>
<tr><td>Cost</td><td>The cost of all rates applied directly to the account holders MBR. Costs applied to other MBRs for reseller billing purposes are not</td></tr>
</table>
</td></tr>
</table>

		included.
	MatchStatus	When the values of a rated item are matched explicitly to a rate rule or to the rules default rate MatchStatus is 1. If there are no explicit matches and the default rate is disabled MatchStatus is 0.
	Variables begin with the $ character followed by the field name. For example assume a row contains the Field 'CallID' with a value of 1 – 'UPDATE mydb SET LastCallID=$CallID' would become 'UPDATE mydb SET LastCallID=1'. String data must prefix the " ' " character before variable name. Assuming FirstName is "IEA's test" - UPDATE mydb SET FirstName=$'FirstName should be used. Using $FirstName would result in SQL error because value contains characters not allowed in an unquoted context and therefore substituted for empty value. Native datetime field translation is not possible – you will have to manually convert any timestamp fields to the proper string format. When "Update Interval" is "Data Query" the data in the last row returned is available in the Update Query -- you may need to order the results of the "Data Query" to properly mark all effected rows as having been rated.	
Re-Rate Query	When defined an option is provided with rating datasource to "re-rate" usage. The defined query generally clears rated data having not yet been rolled into an invoice so it can be re-rated. Normally rerate is incompatible with the billing mode "Usage Billing via Rate History" and should only be used with the "Rate Only / No Billing" mode. If used with rate history based mode the re-rate query would have to take steps to clear rate history usage affected by a rerate.	

Voice Records Data Source

Emerald includes a preconfigured rating data source to enable Call Records from an external source to be easily imported into the Emerald database. This feature operates quite differently than real-time rating processed via RadiusNT/X or the EmerNet traffic collector. The main benefits of using the Voice Record data source is it is simplified to accept external Call Detail information from a variety of sources, per call cost information is available for review by the end user and re-rating of voice records even after they have been applied to an invoice is easily achieved. The disadvantage of using the Voice Record data source this is not a real-time system and therefore not possible to use this data to actively enforce pre-paid data limits as is possible when RadiusNT/X is used to rate Voice records for real-time calling card applications.

Call record import is accomplished using a data import tool similar to Microsoft DTS Wizard/SSIS or third party utility. All call record data is added to the VoiceCalls table located within your Emerald database for processing. The table below describes the VoiceCalls table in detail to assist you in mapping your existing call data files to the Emerald database.

Field	Type	Required	User Editable	Description
VoiceCallID	Integer	N/A	No	Database assigned unique call identifier.
AccountID	Integer	N/A	No	A MBRs service ID the call record is to be billed/associated with. This field is set automatically after the call record is rated.
CallDate	DateTime	Yes	Yes	Starting date and time of the call
Login	String	Yes	Yes	This must match the login field of a MBRs service for billing purposes. If there is no match to a services login field within Emerald the Call record will not be rated. Login is

				typically the calling number/customer DID.
Duration	Integer	Yes	Yes	Total duration in seconds of the call. Note the ending time of a call is considered to be CallDate + Duration. If the call record is being billed on a data rather than time basis you may set Duration to 0 and use Bytes to specify the amount of data transferred.
SessionRef	String	No	Yes	Optional per call session identifier that uniquely references each call record in the external call data.
CalledNumber	String	No	Yes	For origination this is the number dialed. For termination this should be set to a null value or descriptive string such as INCOMING CALL
CallingPort	String	No	Yes	Optional reference of the hardware port used to originate the call
CalledPort	String	No	Yes	Optional reference of the hardware port used to terminate the call
Bytes	Integer	No	Yes	If billing based on data usage this is the number of billable bytes used.
CallType	String	No	Yes	Optional call type typically used as a hint to the rating system to trigger special pricing considerations. Examples of call type include local, long distance, voice mail access, information services…etc.
AcctTerminateCause	Integer	No	Yes	Optional RADIUS Acct-Terminate-Cause compatible session termination reason.
CountryID	Integer	No	Yes	UN Country ID from the Emerald Countries table of the number called (origination). If not specified Emerald can periodically attempt to determine the location setting CountryID on a successful match based on internal geographic information. This requires the 'Determine called location for voice calls' scheduled task be enabled. (Procedure RateVoiceCallsLoc)
StateID	Integer	No	Yes	State ID from the Emerald States table of the number called (origination).). If not specified Emerald can periodically attempt to determine the location setting StateID on a successful match based on internal geographic information. This requires the 'Determine called location for voice calls' scheduled task be enabled. (Procedure RateVoiceCallsLoc)
Location	String	No	Yes	String describing the location of the number called. Location can be as general or specific as necessary / available.). If not specified Emerald can periodically attempt to determine the location at the city level on a successful match based on internal geographic information. This requires the "Determine called location for voice calls" scheduled task be enabled. (Procedure RateVoiceCallsLoc)
ChargeID	Integer	N/A	No	After a call record has been successfully rated and usage charges processed and applied to an account this contains a reference to the usage

				charge. **Do not make changes to this field.**
ProcDate	DateTime	N/A	No	Date and Time this voice record has been successfully rated. If you are importing pre-rated call records that do not need to be rated you may set the ProcDate and Cost fields to signal your records have already been processed.
ErrorCode	Integer	N/A	No	If there was an error rating a call record this contains the error code showing this error. Currently the only error code possible is 1 which means there were no applicable rating rules and no default to determine pricing for a specific call.
Cost	Money	N/A	No	Actual cost to the end user of this call. This field is determined automatically after the rating process has completed. If you are importing pre-rated call records that do not need to be rated you may set the Cost field to the known cost of the call record. When manually configuring cost you must also set a value for the ProcDate field.

When using the Voice Record data source the following steps should be followed to correctly process call records.

1. Import your call detail records into the VoiceCalls table. Database level constraints ensure the same call records are not accidently imported more than once.

2. From the rating data sources menu click the "test" button on the Voice Records item to do a simulation of the rating process to spot check making sure rates are properly configured.

3. From the same menu click "Process" to process all call records. Periodic processing of call records can be automated by clicking the "schedule" button on the data sources listing for Voice Records.

4. Perform an in-depth review of rated call records by reviewing calls and pricing from the MBRs service call search menu of several accounts to ensure proper rating configuration.

5. If corrections need to be made, make any adjustments and click the "Re-Process" button to re-rate all records not already invoiced and then repeat step 4.

6. Once you have ensured proper rating - process usage charges from the Emerald Client / Billing / Usage Charges menu. This step applies usage charges to the MBRs. These charges will appear on the customer's next invoice. This process can be automated by enabling the "Create Usage Charges" scheduled task via the Emerald Admin / Scheduler / Configure Schedules menu. Note the usage charge summary table displays only real-time summaries and does not display information for the VoiceCalls table. Also note that not all pending call detail records may immediately be assigned as charges. This is typically because the call record may fall within a current billing period for a customer and more time needs to pass in order to ensure the user is billed for the completed period. You may override this behavior via the Emerald Admin / Accounting / Settings / Rating Charge Delay & Rating Allow Interim Charges options.

7. If you discover a rating or data error in an account after it has been billed you may delete the adjustment from the MBRs history menu and "Re-Process" per step 5 above. If the adjustment has already been assigned to an

invoice you must first void that invoice and then delete the duplicated usage charge adjustment from the history menu before "re-reprocessing" per step 5 above.

VOICE RECORD REPORTING

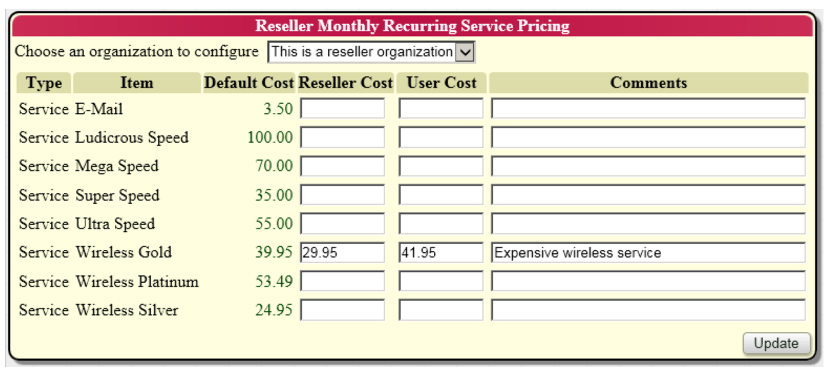
Rated voice records appear for review in the Emerald operator interface from the Call Search option of each accounts MBR service menu. Customers also have the opportunity to review call history from the Emerald customer account center. Additionally you may enable the attachment of detailed call history to invoices and statements by setting the Invoice Report and Statement Report fields of the desired billing groups (Emerald Admin / Billing Groups) to the included invoice_cdr.rpt and statement_cdr.rpt call detail reports.

RESELLERS

This menu enables reseller operators to manage their own groups of customers, invoicing, credit card processing and reporting for their customers. Resellers are then invoiced separately for usage of their customers. This menu provides organization, billing group and reseller service pricing configuration.

Service Pricing

Service pricing allows global administrators to set pricing independent of the service types cost field for both what the reseller is charged per service and what the reseller's customers are charged. Resellers with object access to the "Admin" and "Admin Reseller (Customer)" object group are also allowed to configure the amount charged to their customers however they are not able to modify the amount charged to the reseller.



Reseller Monthly Recurring Service Pricing

Choose an organization to configure: This is a reseller organization

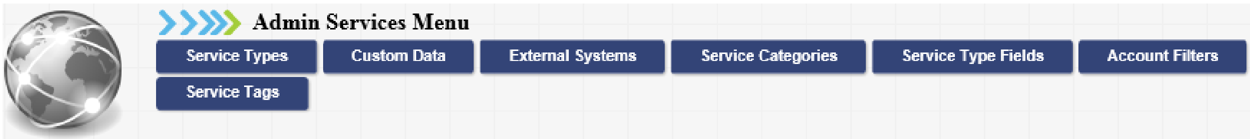
Type	Item	Default Cost	Reseller Cost	User Cost	Comments
Service	E-Mail	3.50			
Service	Ludicrous Speed	100.00			
Service	Mega Speed	70.00			
Service	Super Speed	35.00			
Service	Ultra Speed	55.00			
Service	Wireless Gold	39.95	29.95	41.95	Expensive wireless service
Service	Wireless Platinum	53.49			
Service	Wireless Silver	24.95			

Update

```
The "Admin Reseller" object group MUST NOT be assigned to a reseller's
operator group.
```

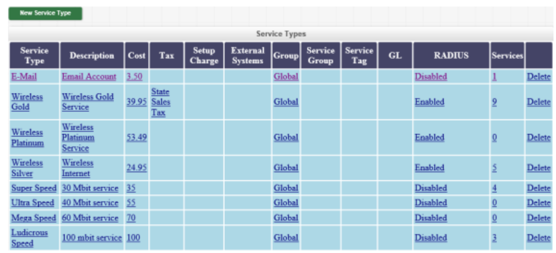
SERVICES

Recurring and nonrecurring services purchased by customers and provisioning options are managed from services menu.



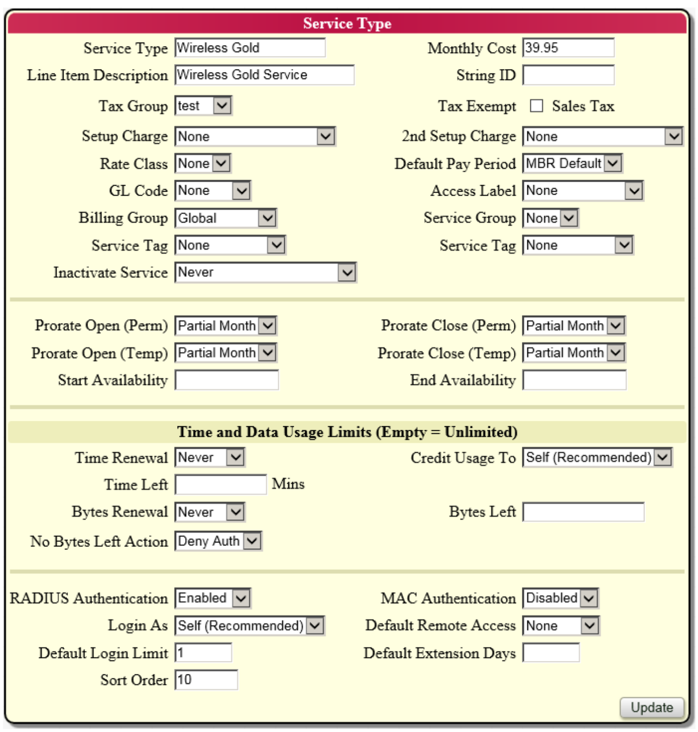
Service Types

Service types define available services for purchase on a recurring or nonrecurring basis. With each service type billing characteristics including base monthly cost, usage charges, taxes, setup charge and service proration are configured. Additionally time and data limits, RADIUS authorization and external system provisioning work to define service level offered by each service type.


New Service Type

Service Types

Service Type	Description	Cost	Tax	Setup Charge	External Systems	Group	Service Group	Service Tag	GL	RADIUS	Services	
E-Mail	Email Account	3.50				Global				Disabled	1	Delete
Wireless Gold	Wireless Gold Service	39.95	State Sales Tax			Global				Enabled	9	Delete
Wireless Platinum	Wireless Platinum Service	53.49				Global				Enabled	0	Delete
Wireless Silver	Wireless Internet	24.95				Global				Enabled	5	Delete
Super Speed	30 Mbit service	35				Global				Disabled	4	Delete
Ultra Speed	40 Mbit service	55				Global				Disabled	0	Delete
Mega Speed	60 Mbit service	70				Global				Disabled	0	Delete
Ludicrous Speed	100 mbit service	100				Global				Disabled	3	Delete



Field	Description
Service Type	Enter the identifying name for the Service Type. This description will be used within the 'Service Type' selection lists throughout Emerald.
Monthly Cost	Recurring base monthly cost charged for this service. The cost entered is always the monthly rate regardless of the intended service pay period. The effective base cost may be overridden by service category, reseller or market tag based pricing or discounting. Where the service type is

	used to provide non-recurring service the monthly cost field is ignored. For non-recurring pricing see Time & Data Charges.
Line Item Description	Enter a longer comment or description to clarify the Service Type. This description will appear on invoice line items of customers who subscribe to this service.
Schedule Cost Change	New base monthly cost to apply to future invoiced billing periods starting "Change Effective" date below after which "Schedule Cost Change" takes precedence over "Monthly Cost". "Changes Effective" applies to billing period covered by the invoice rather than when in time invoice is generated. For example in November new monthly service cost is entered into this field with a "Change Effective" date of March 1st. Later in November a customer with a yearly pay period is invoiced for a year's service Dec thru Nov. In this case when the invoice for a year of service is generated the normally yearly line-item is split into a separate line item for periods covered by each of the two rates. The monthly rate of "Monthly Cost" is charged Dec thru Feb and "Schedule Cost Change" for Mar thru Nov. Similarly if a an account with an anniversary billing cycle and a monthly pay period is normally invoiced for the 15th thru 14th the change is prorated such that "Monthly Cost" is charged for the 15th thru last day of month and "Schedule Cost Change" for first day of new month thru the 14th. Once scheduled cost is entered further changes to "Monthly Cost" are locked out. See change effective below for more information.
Change Effective	This required field is only displayed once a new monthly cost is entered into "Schedule Cost Change" to determine when new cost is to take effect. See "Schedule Cost Change" for more details about how this field influences invoicing. This field should always reference a future date. Two months from the effective date "Monthly Cost" is automatically changed to the value of "Schedule Cost Change" and both "Schedule Cost Change" and "Change Effective" are automatically cleared.
String ID	See Common fields
Tax Group	Select tax group to be used to determine applicable taxes for recurring service. The chosen tax group does not apply to postpaid usage charges associated with the service nor is the group used in conjunction with non-recurring service charges. Taxes for these items are configured with their respective charge types.
Tax Exempt	Enabling a tax exemption indicates any applicable taxes with a matching exemption are not applicable to invoice line items involving this service type.
Setup Charge	Enter applicable one-time set up charge for this service type. Setup charge options are configured as charge types. If a setup charge is selected the charge can be waived during MBR Service account creation. Setup charges are only created during initial service creation.
2nd Setup Charge	Provides an additional setup charge in addition to the above setup charge field. If both setup charges are defined both are billed to the MBR on service creation. The secondary setup charge may be used to itemize multiple setup fees and distinguishing tax and non-tax portions related to account setup.
Rate Class	If this service type is to include a rate structure for separate postpaid time or data based usage charges select the appropriate rate class to assign to this service type.
Default Pay Period	Selects the default pay period to be used on account creation. When "MBR Default" is selected the MBR level pay period discount is used on new service creation. When any other pay period is selected that pay period is used as default service pay period ignoring MBR default.
GL Code	General ledger code to be associated with recurring service charges associated with this service type. Selected GL code does not apply to service related non-recurring fees such as setup charges, postpaid usage fees or non-recurring Time & Data Charges. GL codes for these items are configured with their respective charge types.

<table>
<tr><td>Access Label</td><td>See Common fields</td></tr>
<tr><td>Billing Group</td><td>See Common fields</td></tr>
<tr><td>Service Group</td><td>See Common fields</td></tr>
<tr><td>Service Tag</td><td>Marks service type as being a member of selected service tag. Service tags are used to associate related service types so that they can be referenced as a group by individual market tags.</td></tr>
<tr><td>Inactivate service</td><td>When an individual service within an active MBR is canceled with non-temporary cancellation reason this setting controls how many days after cancellation date the state of the account transitions from a "canceled" to an "inactive" state.

The primary difference between services remaining with canceled vs inactive state is inactive services are eligible for permanent de-provisioning of the underlying service provided to the account holder. For example when inactivated some systems may permanently delete the underlying mail store for an email account. In some cases inactive services may also be eligible to have reserved usernames reused by new customers.</td></tr>
<tr><td>Prorate Open Service</td><td>When a new service is created for the first time or re-opened this controls how proration if necessary is handled.

"Perm" refers to proration when initially opening account or opening from a previous permanently closed service.

"Temp" refers to proration when reopening account from a previously temporarily closed service.

<table>
<tr><th>Prorate</th><th>Description</th></tr>
<tr><td>Partial Month</td><td>This is the recommended default. With this method the new service is pro-rated for the remainder of the accounts billing month charging a 30th of the monthly rate per day of proration.</td></tr>
<tr><td>Full Month</td><td>Charges full month's price for prorated period regardless of number of days prorated.</td></tr>
<tr><td>No Charge</td><td>Charges nothing for prorated period regardless number of days prorated.</td></tr>
</table></td></tr>
<tr><td>Prorate Closing Service</td><td>When closing a service this option determines the credit issued over remainder of the customer's cycle.

"Perm" refers to proration when permanently closing service by choosing a permanent cancel reason.

"Temp" refers to proration when temporarily closing service by choosing a temporary cancel reason.

<table>
<tr><th>Prorate</th><th>Description</th></tr>
<tr><td>Partial Month</td><td>This is the recommended default. With this method closed services are invoiced thru service closing date. Services are not invoiced for any remaining days of billing month or any subsequent months included with normal service pay period.

Partial month prorates are calculated using normal daily rate of 1/30th monthly rate.

For example if a service with a yearly pay period is closed 1 month and 5 days into a 1 year pay period the service is invoiced for 1 month and 5 days.</td></tr>
<tr><td>Full Month</td><td>With this method closed services are invoiced for the entire billing month regardless of when within the billing month closing date occurs. Services are not invoiced for any remaining full billing months included with the</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td></td><td>services normal pay period.

For example if a service with a yearly pay period is closed 1 month and 5 days into a 1 year pay period the service is invoiced for 2 full months.</td></tr><tr><td>No Credit</td><td>With this method closed services are invoiced for the entire service pay period regardless of when within the pay period closing date occurs.

For example if a service with a yearly pay period is closed 1 month and 5 days into a 1 year pay period the service is invoiced for 12 full months.</td></tr></table></td></tr>
<tr><td>Start Availability</td><td>A starting date when Operators may start using this service type. Before the starting date this service type is not available when creating a new account.</td></tr>
<tr><td>End Availability</td><td>An ending date after which Operators may no longer use this service type when creating new accounts. The ending date has no effect on accounts already assigned to this service type.</td></tr>
<tr><td>Time Renewal</td><td>This feature determines how often the services time left field is replenished. Available options are monthly based on services billing day, daily after midnight of each new day or never.

When replenished time may only be renewed up to the time left field below regardless of previously unused time unless an accumulation limit is configured below.

Renewal depends on the setting "Emerald Admin" / "Accounting" / "Settings" / "Time Left Update" to be enabled.</td></tr>
<tr><td>Credit Usage To</td><td>Controls service to which time and data monthly and daily usage renewals are applied.

<table><tr><th>Credit Usage</th><th>Description</th></tr><tr><td>Self</td><td>Time or data usage renewals are transferred to the service. This is normal recommended setting.</td></tr><tr><td>Parent Service</td><td>Time or data usage renewals are transferred to the parent service of this service. Typically used where service type is an "add-on" service intended to modify properties of the parent.</td></tr></table></td></tr>
<tr><td>Time Left</td><td>Indicates default quantity of system access time (in minutes) service will initially have available at start of service or upon renewal at start of each billing month or day.

Enforcement of time left requires the RadiusNT/X Advanced menu option "(Auth) Time & Data banking" to be enabled from the RadiusNT/X administrator.</td></tr>
<tr><td>Rating Time Left</td><td>Rating time left field is a completely separate optional setting and limit from time left field above enabling time consumption to be controlled by rating engine. This is useful if it should be necessary to offer time limited accounts with "free periods" where consumption limit is not counted or counted at a variable rate based on time of day or calendar.

The rating time left field only appears when a rate class has been selected within this service type. If used corresponding rate should be configured with a consumption unit of "Service Time Left".</td></tr>
<tr><td>Bytes Renewal</td><td>This feature determines how often the services data left field is replenished. Available options are monthly based on services billing day, daily after midnight of each new day or never.

When replenished bytes may only be renewed up to the bytes left field below regardless of previously unused data unless an accumulation limit is configured below.

Renewal depends on the setting "Emerald Admin" / "Accounting" / "Settings" / "Time Left Update" to be enabled.</td></tr>
<tr><td>Bytes Left</td><td>Indicates default quantity of upload + download data consumption in bytes service will initially have available at start of service or upon renewal at start of each billing month or day.</td></tr>
</table>

<table>
<tr><td></td><td>Enforcement of data left requires the RadiusNT/X Advanced menu option "(Auth) Time & Data banking" to be enabled from the RadiusNT/X administrator. Enforcement also requires at least one of the following:

• Access servers support WISPr-Session VSAs or equivalent and RadiusNT/X advanced menu option "(Auth) Limit data left using WISPr-Session VSAs" is enabled.

• Access servers support RADIUS dynamic authorization, Interim accounting is transmitted regularly from access server and session manager is enabled and configured to enforce data consumption limits.</td></tr>
<tr><td>Rating Bytes Left</td><td>Rating bytes left field is a completely separate optional setting and limit from bytes left field above enabling data consumption to be controlled by rating engine. This is useful if it should be necessary to offer data limited accounts with "free periods" where consumption limit is not counted or counted at a variable rate based on time of day or calendar.

The rating bytes left field only appears when a rate class has been selected within this service type. If used corresponding rate should be configured with a consumption unit of "Service Data Left".</td></tr>
<tr><td>No Bytes Left Action</td><td>Manages outcome of RADIUS authentication request when an account has consumed all "bytes left". This setting applies only to "Bytes Left" and does not affect "Rating Bytes Left" where similar configuration is managed separately via rating configuration.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Deny Auth</td><td>Typical default setting. When account bytes left reaches 0 and "time and data banking" enabled within Advanced menu of RadiusNT/X administrator RADIUS authentication fails.

When Emerald session manager is used and bytes left enforcement enabled within session manager configuration sessions exceeding data left allocation are eligible for disconnect.</td></tr>
<tr><td>Allow Auth</td><td>When account bytes left reaches 0 authentications are allowed to succeed despite consumption of allocated usage. Once reached any reply attributes applied to failure cause "No Time/Data Remain" is merged into Access-Accept response.

Example where "Allow Auth" would be used is in creation of policy where user's bandwidth allocation is significantly reduced once they have consumed data allowance. The user is allowed normal access to the network with additional restrictions.

If session manager is used and one or more authorization attributes modified via "No Time/Data Remain" then enforcement of authorization change as a result of exceeding limit requires session manager setting "Enforce Authorization Change" to be enabled. The normal "Enforce Bytes Left" setting is not used and does not apply in this case. If necessary disconnects are automatically issued when transitioning from data to no data or no data to data to reflect current authorization status.

Behavior of this setting differs from the result of applying one or more attributes from failure cause "No Time/Data Remain" and using "Deny Auth" in the following ways:

• When "Allow Auth" normal response attributes are merged with "No Time/Data Remain" attributes.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td></td><td>When "Deny Auth" only "No Time/Data Remain" attributes are transmitted. No normal response attributes are processed or sent.
When "Deny Auth" reaching limit is treated as authentication failure even though RADIUS Access-Accept message is transmitted. The request is logged as an authentication failure and not treated as an "authorized" session. Unauthorized status excludes session from being counted for concurrency enforcement or from being processed by session manager for any reason.

When "Allow Auth" sessions reaching limit are treated as a successful authorization subject to all applicable RadiusNT/X and session manager enforced constraints.</td></tr></table></td></tr>
<tr><td>Rollover Accumulation Limit ***</td><td>When time or data renewal is configured to occur on a monthly or daily basis any unused time or data at the time of renewal is carried forward upon renewal up to the configured accumulation limit. If no limit is configured renewal is limited to the renewal quantity.</td></tr>
<tr><td>RADIUS Auth</td><td>When "Enabled" any services using this service type may authenticate via RADIUS using service level credentials. It is no longer necessary to assign at least one RADIUS authorization attributes to enable RADIUS authentication.

When "Disabled" any services using this service type may not authenticate via RADIUS using service level credentials. If the service is a child of a parent service where RADIUS authentication is allowed then any RADIUS attributes configured for this service type configured to apply to parent service are still honored regardless of RADIUS authentication setting.</td></tr>
<tr><td>MAC Auth</td><td>When "Enabled" services with this service type are able to authenticate using MAC address.

To facilitate MAC authentication the services login field should be set with users MAC address and password field left blank. MAC authentication password configured within the access server is then entered into "MAC Auth Password" field of the RADIUS access server configuration. If no MAC password can be configured within access server the "MAC Auth Password" field should be set to keyword "ANY" to bypass password checking. Format of the MAC address entered into service login field should contain only MAC address without any format delimiters regardless the format of MAC addresses transmitted by access server within RADIUS access-request.

When MAC authentication is performed the Calling-Station-Id field if available is also checked to confirm agreement with Username and MAC password. If there is no agreement the authentication fails. If a standard username and password is configured within a service where MAC auth has been enabled user is still able to authenticate normally and MAC authentication is automatically not performed.

When "Disabled" the MAC authentication feature described above is disabled. Services may authenticate only with username and password.</td></tr>
<tr><td>Login As</td><td>Login As determines account that is to be used to provide service when a user logs on using their service username and password. Most commonly used and recommended setting is "Self".

<table><tr><th>Login As</th><th>Description</th></tr><tr><td>Self</td><td>When authenticating with username and password the service matching the entered credentials is used.</td></tr><tr><td>Parent Service</td><td>When authenticating with username and password the parent service of the child service matching entered credentials is used. In this case child service is essentially leveraged as an "Alias" of the parent service.</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td></td><td>Authorization attributes, consumption limits, concurrent login enforcement and accounting all reflects the parent service rather than child service used for authentication.

This feature is typically used to support "shared" accounts where each user is given their own login and password but concurrent usage limits and or time/data allocation is linked and limited across all users.

To properly support this feature access servers should support the "Class" attribute. This is necessary for RADIUS accounting data to be properly attributed to the parent account even though username is of child account. Without Class support accounting will assigned to the child preventing proper attribution. If access servers do not support class attribute and this feature is used consider enabling "Virtual class attribute" support for local requests from Advanced menu of RadiusNT/X Administrator.</td></tr></table></td></tr>
<tr><td>Default Remote Access</td><td>Default access level granted to service accounts for access to customer account center. The default setting is assigned to the service upon initial service creation and may later be customized on a per-service basis.

<table><tr><th>Access</th><th>Description</th></tr><tr><td>Manager</td><td>Grants user full account access to customer center subject to administratively configured access restrictions. Access granted includes access to billing history, ability to create credit card payments, recharge from prepaid vouchers, purchase blocks of time/data, create incidents, upgrade or downgrade service levels, provision new services, review network usage of all services within MBR, change of address, password and cancel services.</td></tr><tr><td>Service</td><td>Access to customer center is limited to the logged on service. No MBR level features are offered. Users may only view network usage of their service account, change password, create an incident, purchase time or data and recharge their account.</td></tr><tr><td>None</td><td>Remote access using this account is disabled.</td></tr></table></td></tr>
<tr><td>Default Login Limit</td><td>Default number of active login sessions user is allowed to have opened at the same time.

Enforcement of concurrent login restrictions requires at least one of the following:
Concurrency enforcement during user authentication by enabling "(Auth) Concurrency control" from advanced menu of RadiusNT/X Administrator.
Session manager installed and configured with "Enforce Concurrency Control" enabled to enforce concurrent access restrictions post-authentication. Access servers must support RADIUS dynamic authorization to use session manager.
The default setting is assigned to the service upon initial service creation and may later be customized on a per-service basis.</td></tr>
<tr><td>Default Extension Days</td><td>Default permanent extension assigned to recurring renewal based services. Extensions allow services to continue to operate for set number of days after service expiration.

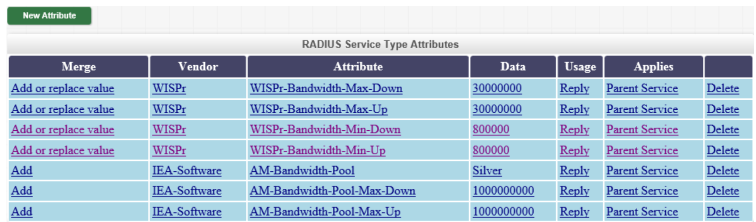
If set the global or group level Accounting menu setting "Default Expire Grace Period" is overridden. A temporary extension adding to the existing service expiration may also be set from within the MBR to allow customers more time once their account has expired on a temporary basis. MBR level temporary extension is automatically cleared the next time the account is invoiced.

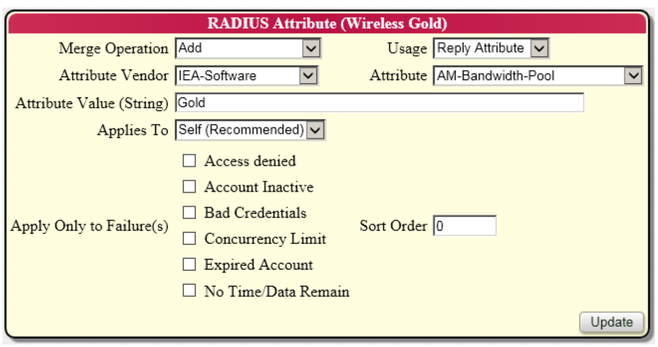
The default setting is assigned to the service upon initial service creation and may later be</td></tr>
</table>

	customized on a per-service basis.
Sort Order	See Common fields

RADIUS Service Type Attributes

During RADIUS authentication of user sessions authorization attributes are transmitted to access server defining session properties and limits unique to each user. For example users allowed session duration may be limited to service period currently paid or bandwidth allocation limited based on the users chosen monthly access plan.





Field	Description
Merge Operation	Merge operation determines how this attribute will interact with existing authorization attributes queued before it. Ordering in which attributes are processed can affect outcome of merge operations and may also affect meaning of attributes transmitted. When defining order dependent attributes such as an ACL or sequencing dependent on outcome of previous merge operations it is recommended sort order be set to enforce ordering explicitly. In addition to service type level authorization attributes, additional attributes may be merged from a variety of sources during user authentication. Those sources in the order they are merged are provided in the table below. **Order / Source** 1st – Service type attributes 2nd – Service type attributes added by presence of child services where one or more of the child's service type RADIUS attributes are set "Applies To" = "Parent Service". 3rd – Per account service level custom attributes 4th – Attributes associated with active market tags 5th – Attributes associated with inventory assigned to service Listing of all supported merge operations is found below. The typical recommended merge operation is "Add" which simply appends an attribute to the set of outgoing authorization attributes. **Option / Description**

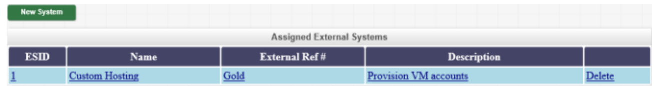
<table>
<tr><td></td><td><table>
<tr><td>Add</td><td>Adds a new RADIUS attribute of type "Attribute Vendor" and "Attribute" containing the value "Attribute Value".</td></tr>
<tr><td>Add or replace value</td><td>Similar to Replace value except that if no attributes match the attribute containing the new value is added.</td></tr>
<tr><td>Delete</td><td>Delete any attribute matching the "Attribute Vendor" and "Attribute" fields.</td></tr>
<tr><td>Delete matching</td><td>Delete any attribute matching the "Attribute Vendor" and "Attribute" fields also having a matching "Attribute Value"</td></tr>
<tr><td>Replace value</td><td>For every RADIUS attribute matching "Attribute Vendor" and "Attribute" replaces its current value with contents of "Attribute Value".</td></tr>
</table></td></tr>
<tr><td>Usage</td><td>Usage determines whether attribute will be transmitted as authorization response or checked against authentication request. Typical recommended setting is "Reply Attribute".
<table>
<tr><th>Usage</th><th>Description</th></tr>
<tr><td>Reply Attribute</td><td>Attribute will be transmitted normally as an authorization attribute included with RADIUS Access-Accept response.</td></tr>
<tr><td>Check Attribute</td><td>Attribute and value is checked against Access-Request attributes transmitted with RADIUS authentication request. If request attribute of the same type as check attribute is present then its value must match check attributes value or authentication fails. If multiple check attributes are defined of the same "Attribute Vendor" and "Attribute" then one of the check attribute values must match authentication request.</td></tr>
</table></td></tr>
<tr><td>Attribute Vendor</td><td>Select the appropriate attribute vendor from vendor selection list to change attribute space to selected vendor. Once attribute vendor has changed "Attribute" list below is automatically updated to reflect attributes available for the vendor. Available vendors and attributes are managed from the RADIUS vendors menu.</td></tr>
<tr><td>Attribute</td><td>Select the appropriate Attribute from the attribute selection list. Only the attributes for the above selected Vendor will be available in the pick list.</td></tr>
<tr><td>Attribute Value</td><td>Enter desired attribute value corresponding to selected attribute above.</td></tr>
<tr><td>Applies To</td><td>Determines which service this attribute is assigned. Typical recommended setting is "Self".
<table>
<tr><th>Applies To</th><th>Description</th></tr>
<tr><td>Self</td><td>Attribute will be applied directly to the service account</td></tr>
<tr><td>Parent Service</td><td>Attribute will be applied to the services parent service</td></tr>
</table></td></tr>
<tr><td>Apply Only to Failure(s)</td><td>When no checkboxes are selected the attribute is processed normally.

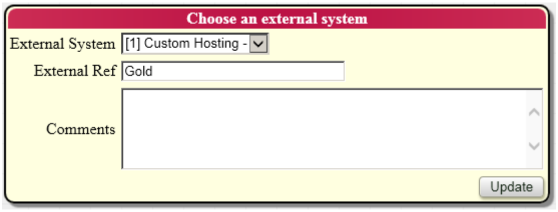
When one or more checkboxes are selected the attribute is not processed normally and shall not be transmitted with normal reply attributes. Should authentication fail due to a selected cause rather than responding normally with authentication failure (Access-Reject) the authentication is accepted (Access-Accept) and only those attributes where checkbox associated with failure cause is transmitted as authorization attributes. This feature is typically used to grant limited access to users as notification of account related problems.

For example assume a user's account has expired. Rather than being completely denied access the attribute Framed-Pool=expired is transmitted signaling NAS to assign an IP from a special pool where a captive portal is used to inform user of an expired account and enable them to make a payment to restore service from customer account center.</td></tr>
<tr><td>Sort Order</td><td>Determines order attributes are processed and sent. Attributes having lower sort order are sent before attributes with higher sort orders.</td></tr>
</table>

Assigned External Systems

To enable external provisioning assign one or more external systems to this service type.

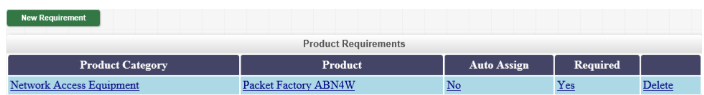


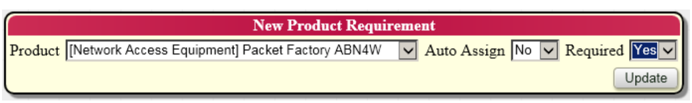


Field	Description
External System	Selection of appropriate external system for provisioning accounts of this service type.
External Ref	This field is external system dependent sometimes used to signal service type specific profile in case where a single external system is used by multiple service types.
Comments	Additional information about this external system.

Product Requirements

If accounts with this service type require hardware or network address to be assigned from inventory those requirements may be configured here. Once a requirement is configured the operator is alerted to any unfulfilled assignments when viewing the account or viewing related exception reports. Only inventory products from product sources having source type "IP reservation" or "Stocked Rental" are available for configuration as a product requirement.



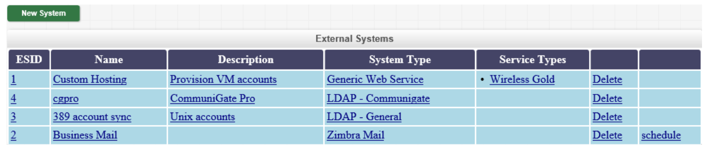


Field	Description
Product	An Inventory product to be allocated to services of this service type.
Auto Assign	Enables automatic assignment of product from inventory to service without operator intervention. This feature can only be used when assigning network addresses to account and cannot be used to assign physical products.
Required	When "Yes" the operator is alerted to the need to assign item from inventory when viewing the service and an item of the selected type is not currently assigned to the account.

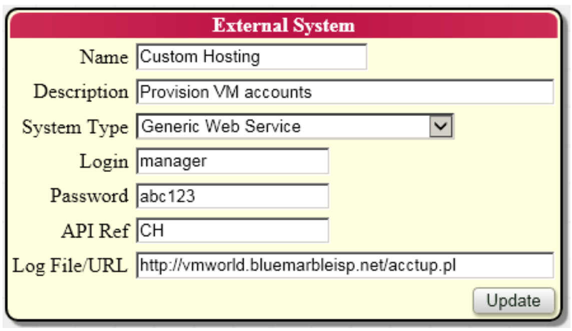
Account Configuration

One or more service templates may be assigned to customize service management from perspective of operators, signup and customer account center. Service templates are generally used in implementation of custom add-on functionality and may not be available by default.

External Systems



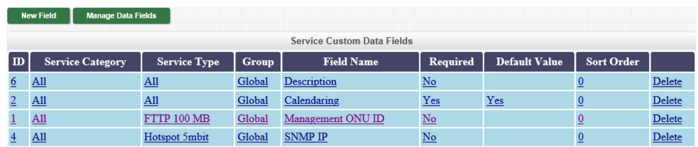
Emerald allows for the configuration of external systems to synchronize customer account information with other types of systems such as email servers, hosting panels, custom processing, authentication systems, database and LDAP account synchronization. In order to directly support provisioning to specific external systems export configuration or database/LDAP schema sync must first be created. Configuring support for currently unsupported external systems is outside the scope of this documentation and product support.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter a name uniquely identify the external system. This field is used to associate some external systems by name (LDAP synchronization) rather than External System ID (ESID).</td></tr>
<tr><td>Description</td><td>Text describing the purpose of this external system in detail. Description is used for informational purposes only and is visible when associating service types to external systems.</td></tr>
<tr><td>System Type</td><td>Most system types directly reflect the external system to be synchronized with following exceptions.
<table>
<tr><th>System Type</th><th>Description</th></tr>
<tr><td>External</td><td>Used by external systems providing their own synchronization from Emerald.</td></tr>
<tr><td>Export</td><td>File or http export of Emerald account information. Requires a compatible export format to be selected.</td></tr>
</table></td></tr>
<tr><td>Export Format</td><td>Select the appropriate export format from the available options presented.</td></tr>
<tr><td>Export Mode</td><td>For "Export" based system types where export format is file based the following file handling options are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Append</td><td>Existing export file if it exists will be added to instead of replaced with each export operation. If the file does not already exist a new file will is created.</td></tr>
<tr><td>Overwrite</td><td>Exported file will be rewritten with each data export. Any previous data is replaced.</td></tr>
</table></td></tr>
<tr><td>Mail Host</td><td>Enter the name of the mail server accepting delivery of mail to these accounts if supported or required by selected external system.</td></tr>
<tr><td>Login
Password</td><td>Enter the login and password values, respectively, for export system to login remotely for external system processing, if necessary. Currently these values are only used within Emerald in HTTP(S) post mode to login to remote web servers.</td></tr>
<tr><td>Log File/URL</td><td>Enter the file name or URL of where Emerald should send its export data depending on selected system type and export format.</td></tr>
</table>

```
External systems requiring scheduling for periodic synchronization display a
"Schedule" link in the external system list to create a recurring schedule
for synchronization.
```

Service Custom Data Field



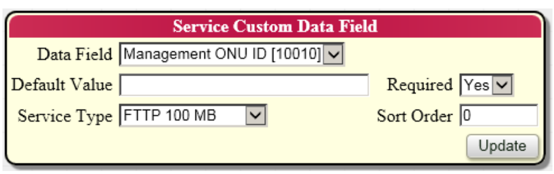
New Field | Manage Data Fields

Service Custom Data Fields

ID	Service Category	Service Type	Group	Field Name	Required	Default Value	Sort Order	
6	All	All	Global	Description	No		0	Delete
2	All	All	Global	Calendaring	Yes	Yes	0	Delete
1	All	FTTP 100 MB	Global	Management ONU ID	No		0	Delete
4	All	Hotspot 5mbit	Global	SNMP IP	No		0	Delete

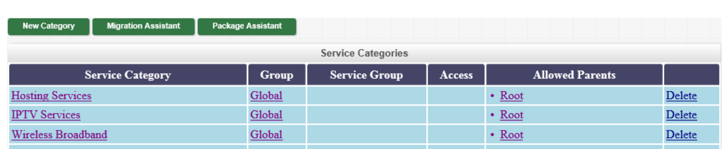
Service custom data enables additional operator configured fields to be tracked with each service account. When configured custom data fields appear within "edit service" form of applicable services. Custom data is also displayed when viewing a service from "Show service" menu as well as custom data searches from Emerald client accounts search menu.

Service Custom data fields can be informational used for tracking and reporting or used to supply additional information to external systems for provisioning or rating. In addition to custom data fields managed within this menu additional service level custom data fields may be applied to services depending on external systems assigned to the accounts service type.



Field	Description
Data Field	Reflects the custom data field to be added. Selection list of available data fields are configured from the "Manage Data Fields" submenu of Emerald Admin / Services / Custom Data.
Default Value	Sets the default value to be set when a new service account is created.
Required	Requires an operator to enter a value for this custom data field before they are able to save changes to the service form.
Billing Group	See Common fields
Service Type	When custom field is only to be tracked for those services of a specific service type select the appropriate type. When service type is "All" the custom data field is included across all services within Emerald.
Sort Order	Controls ordering custom data fields are presented in the edit service form in ascending order.

Service Categories



New Category | Migration Assistant | Package Assistant

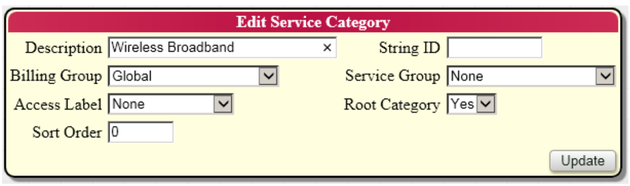
Service Categories

Service Category	Group	Service Group	Access	Allowed Parents	
Hosting Services	Global			• Root	Delete
IPTV Services	Global			• Root	Delete
Wireless Broadband	Global			• Root	Delete
Wireless Add-On	Global			• Wireless Broadband	Delete

Related service types are grouped together into one or more service categories. For example service types: wireless gold, wireless platinum and wireless silver are all used to provide fixed wireless Internet and therefore each is associated with wireless broadband service category. When new services are created operators first assign a service category before choosing a specific service type within the category. Once a service has been created it may only upgrade or downgrade to any service types within the assigned category.

Service categories offer the following features:

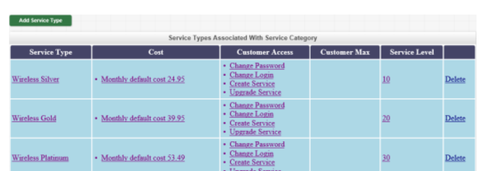
- Improved organization when managing large number of service types
- Service level upgrade and downgrade paths for operators and customer self-management
- Customer access and provisioning limits for customer self-management
- Tiered pricing based on quantity of services assigned to account
- Parent/child service hierarchies for value added services or specialization of parent service

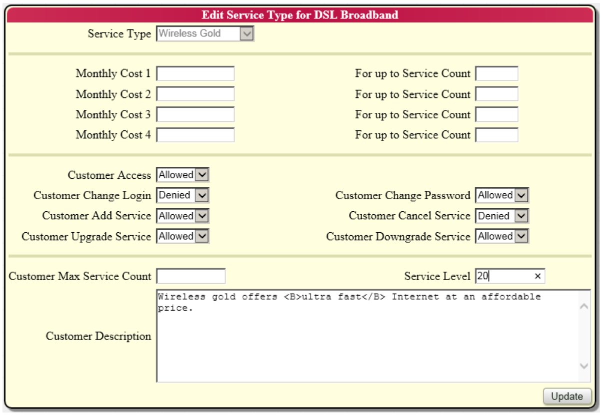


Field	Description
Description	Label uniquely describing the service category. Presented throughout Emerald in service category selection lists.
String ID	See Common fields
Billing Group	See Common fields
Service Group	See Common fields
Access Label	See Common fields
Root Category	When "Yes" this service category may be used when creating new services that are not children of other pre-existing services. When "No" this service category can only be used when creating child services under a pre-existing service having a service category authorized by Allowed Parent Service Categories configured below.
Sort Order	See Common fields

Service Types Associated With Service Category

Once a service category is created one or more service types can be added to the service category.

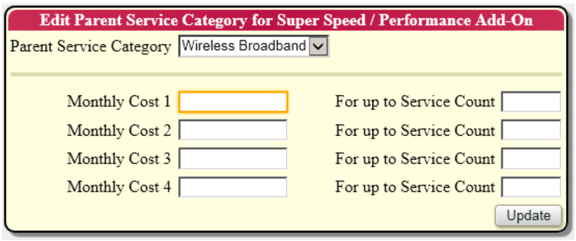




Field	Description
Service Type	Service type to be associated with this service category. (See "Admin" / "Services" / "Service Types")
Monthly Cost / Service Count ***	Overrides service type monthly cost. When up to service count is set monthly cost applies to the first count of services having a matching service type sharing a common parent service if any. If count is not set cost applies to all (remaining) services not previous covered. For example the service type "Email" is configured as follows: 1. Cost 0.00 for up to 5 services 2. Cost 1.00 for up to 10 services 3. Cost 2.00 (service count field left blank) 20 accounts having service type "Email" are configured as children of a common parent business Internet access service. Of the 20 accounts first 5 are priced at 0.00. Next 5 after that are priced at 1.00 and remaining 10 are priced at 2.00.
Customer Access	When "Allowed" customers are allowed to manage services of matching service type and category from the customer account center when customer service has "manager" access.
Customer Change Login	When "Allowed" and "manager" remote access is enabled customers are allowed to change login names of accounts from within the customer account center.
Customer Change Password	When "Allowed" customers are able to change their services access password. If "manager" remote access is enabled for the service then customer may change password of any service within their MBR where customer change password is "Allowed".
Customer Add Service	When "Allowed" customers with "manager" remote access may add additional services of this type and category to the same parent service.
Customer Cancel Service	When "Allowed" customers with "manager" remote access enabled are allowed to cancel services of this type and category from the customer account center. If this setting is "Denied" yet the customer is granted the ability to cancel their entire MBR then all subsequent services including services where this field is set "Denied" will be effectively canceled.
Customer Upgrade Service	When "Allowed" customers with "manager" remote access enabled are able to change account service type to another service type within the same service category having a higher service level where customer access is

	"Allowed".
Customer Downgrade Service	When "Allowed" customers with "manager" remote access enabled are able to change account service type to another service type within the same service category having a lower service level where customer access is "Allowed".
Customer Max Service Count	Maximum number of accounts having "Service Type" the customer is allowed to add from the customer center.
Customer Service Level Type	Limits service type upgrade or downgrade options to those service types within service category having a matching level type. This restriction applies to accounts managed from customer center. See service level types below for more information.
Service Level	Numeric value representing the relative service level of a given service type compared to other service types of the service category. Lower service levels represent lower capability generally cheaper service while higher service levels represent the most capability and highest cost service.
Customer Description	This field is displayed within customer center when upgrading or downgrading service. Description should include full outline of service including pricing, relevant access levels and restrictions. HTML tags may be used to customize presentation.

PARENT DEPENDENT PRICING



Parent dependent pricing is a specialization of pricing described above (Monthly Cost / Service Count ***) for service types associated with service categories except service category of the accounts parent service is also considered when determining cost.

For example a "super speed" add-on service is applied as a child account of a "wireless broadband" account. This same "super speed" add-on is also added as a child of a separate "FTTP broadband" service. When added to "wireless broadband" cost of "super speed" is 20.00. When added to "FTTP broadband" cost of "super speed" is 30.00.

Parent dependent pricing takes precedence over the service categories service pricing however both sets of pricing rules are still fully applicable. This means should parent dependent pricing specify a ceiling for example the first service is free with no other price tiers then any overflow not captured by parent dependent pricing would be based on service pricing of service category if present.

SERVICE TYPE ACCESS CONDITIONS

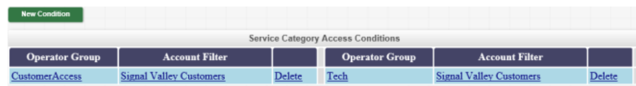
Operation of service type level access conditions is identical to service category access conditions except the effect is at the level of service type availability within service category rather than service category as a whole.

Allowed Parent Service Categories

This feature enables new services to be added as child accounts of existing parent services when the parent's service category is added as an allowed parent.

Child services are generally useful for packaging value-added accounts under primary service account or specializing bandwidth or data allocations of the parent account.

Service Category Access Conditions

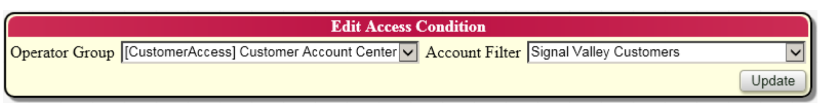


Access conditions work to restrict service categories that would normally available to operators based on matching aspects of MBR such as service location, payment method or active market tags. Restrictions are managed via account filters.

Access conditions are defined on a per operator-group basis. If multiple account filters are assigned to the same operator group than all account filters are combined such that any exclusionary rule across applicable filters results in exclusion of service category regardless of presence of one or more matching rules.

Access conditions are normally restricted to limiting access to service categories. Matching of an access condition does not override any pre-existing constraints such as billing group membership, access label assignment or root / allowed parent relationship hierarchies.

An exception exists when Operator Group "CustomerAccess" is selected in order to apply access condition to users managing their accounts via customer account center. The existence of a matched access condition for a service category with "customer access" and "allow root" enabled enables service category to be made available for customers to add new root services.



Field	Description
Operator Group	Operator Group this access condition is applicable.
Account Filter	Account filter representing fields within the MBR to be matched. If None is selected the condition is unconditionally matched.

Service Type Fields

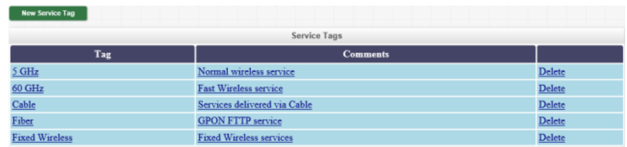
Per service type service level field visibility settings are configured from this menu. Note that only subset of fields that can be applied to a specific service are included. This generally includes any configurable fields within the MBR's service menu of an account. See Field Visibility for more information.

Account Filters

Filters are used to manage service category and service type availability within a service category. See [Account Filters](#) in the General menu for more information.

Service Tags

When assigning [service types to service categories](#) service level types are used in conjunction with service level to limit upgrade or downgrade options to those compatible with customers' existing service from the customer account center.



New Service Tag

Service Tags

Tag	Comments	
5 GHz	Normal wireless service	Delete
60 GHz	Fast Wireless service	Delete
Cable	Services delivered via Cable	Delete
Fiber	GPON FTTP service	Delete
Fixed Wireless	Fixed Wireless services	Delete

For example service category "Wireless Internet" contains following service types:

Service Type	Level	Service Tag
Wireless Bronze	100	5 GHz
Wireless Silver	200	5 GHz
Wireless Gold	300	5 GHz
Wireless Platinum	1000	60 GHz
Wireless Platinum Ultra	1100	60 GHz

Users managing existing "Wireless Silver" service from customer account center have the option of downgrading to bronze level service or upgrading to gold level service. Platinum and platinum ultra are not available to Wireless bronze, silver or gold customers as they are assigned a different service level tag.

Customers with "Wireless Platinum" service have the option only of upgrading service to platinum ultra. Bronze, silver and gold are not available to platinum customers.

Upgrade and downgrade restrictions apply exclusively to the customer center and do not affect an operator's ability to upgrade or downgrade customers between level tags from the Emerald client interface.

Service tags are additionally used as a matching condition for market tags to assist in matching of related service types. For example two service tags are created 'Fixed Wireless' and 'Fiber' representing services provided using respective access technologies.

Service Type	Service Tag
Wireless Gold	Fixed Wireless
Wireless Silver	Fixed Wireless
Fiber 500	Fiber
Fiber 1000	Fiber

Once service tags are created each [Service Type](#) related to 'Fixed Wireless' would be edited and service tag field set to 'Fixed Wireless'. The same process is repeated for 'Fiber' service.

Finally [Market Tags](#) are configured able to match any service type related to 'Fixed Wireless' or 'Fiber' by selecting the 'Fixed Wireless' or 'Fiber' from the 'Service Tag' field of the market tag.

Field	Description
Description	Unique label describing level type. Value is displayed when selecting level types when managing service type assignments at the service type and service category level.
Comments	Informational field to store notes or instructions about the use of this level type
Sort Order	See [Common fields](#)

PREPAID CARDS

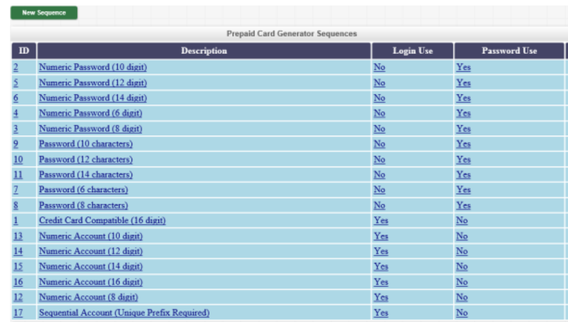
Prepaid vouchers offer simplified means for customers to purchase and access the services you provide.

The following prepaid features are supported:

Feature	Description
Direct Use Accounts	These types of accounts allow the user to directly access services using the login and password provided on the pre-paid card without having to go through an initial sign-up process.
Signup Server	The customer signs up electronically -- allowing the collection of the customer information such as name, address, choice of access plans as well as customized access login and password funded by pre-paid card.
Rechargeable	Existing accounts may be "re-charged" by additional pre-paid cards.
Integrated Batch Generator	Customizable sequence generator for card numbers and password provide endless possibilities for designing your own card generation algorithms with easy access to a cryptographic quality source of random characters.
Batch Types	Provide for stored profile configuration of a prepaid batch so that similar batch creation runs can easily be executed in the future.
Data Export	Prepaid batches are easily exportable in CSV or XML forms.
Batch Management	After a batch is created it can be modified or suspended – additionally utilization statistics are available from the prepaid batches menu.
Isolated Organizations	Prepaid cards created for use with one organization are not useable by members of a different organization.
Customer Interface	Customer center allows the user to automatically purchase additional services, open support tickets and provision new accounts using pre-paid and or a credit cards.
Limited Shelf Life	Prepaid batches can be configured such that cards having not been used over a period of time automatically expire.
Enforce Access Limits	Expiration, session time limits, concurrent access limits and currency based rating required for advanced services such as prepaid telephone cards are possible with

	Emerald and its integrated pre-paid card management system.

Prepaid Sequences



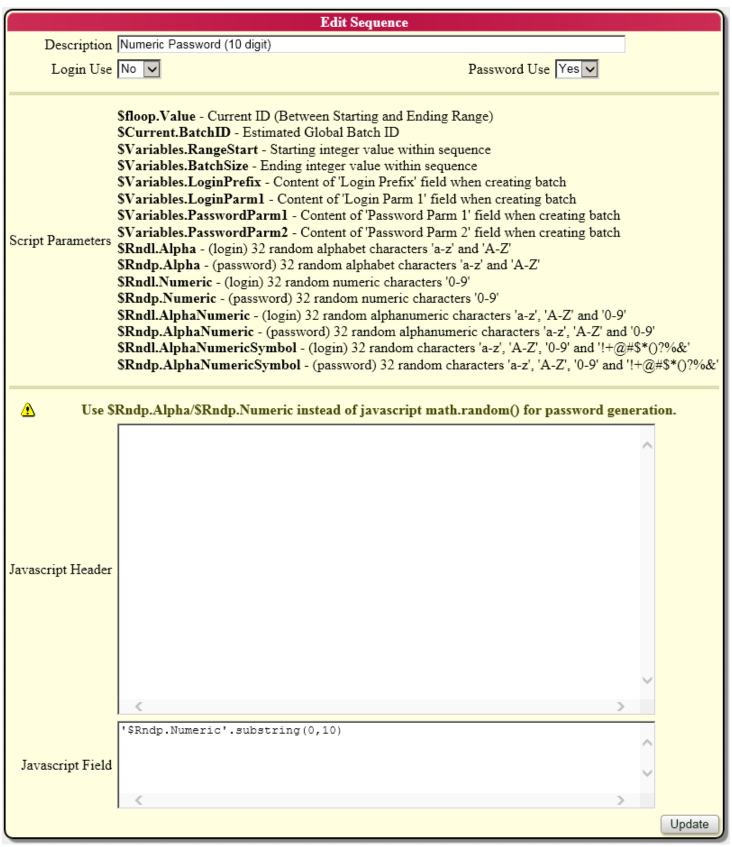
New Sequence

Prepaid Card Generator Sequences

ID	Description	Login Use	Password Use
2	Numeric Password (10 digit)	No	Yes
5	Numeric Password (12 digit)	No	Yes
6	Numeric Password (14 digit)	No	Yes
4	Numeric Password (6 digit)	No	Yes
3	Numeric Password (8 digit)	No	Yes
9	Password (10 characters)	No	Yes
10	Password (12 characters)	No	Yes
11	Password (14 characters)	No	Yes
7	Password (6 characters)	No	Yes
8	Password (8 characters)	No	Yes
1	Credit Card Compatible (16 digit)	Yes	No
13	Numeric Account (10 digit)	Yes	No
14	Numeric Account (12 digit)	Yes	No
15	Numeric Account (14 digit)	Yes	No
16	Numeric Account (16 digit)	Yes	No
12	Numeric Account (8 digit)	Yes	No
17	Sequential Account (Unique Prefix Required)	Yes	No

Sequences generate card login and password fields used in the creation of a prepaid batch. Formatting of generated login and password fields are based on the web browsers JavaScript parser allowing you to design custom sequences using the JavaScript language. Several commonly used formats for login and password sequence generation are included with Emerald.

When creating login sequences it is important to make sure login generated is unique across all prepaid batches in the system. If a duplicate login is generated the prepaid batch creation process fails. When creating password sequences avoid generating passwords which follow a guessable pattern by using provided secure random variables.

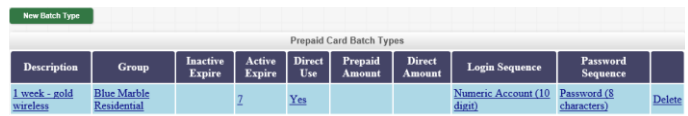


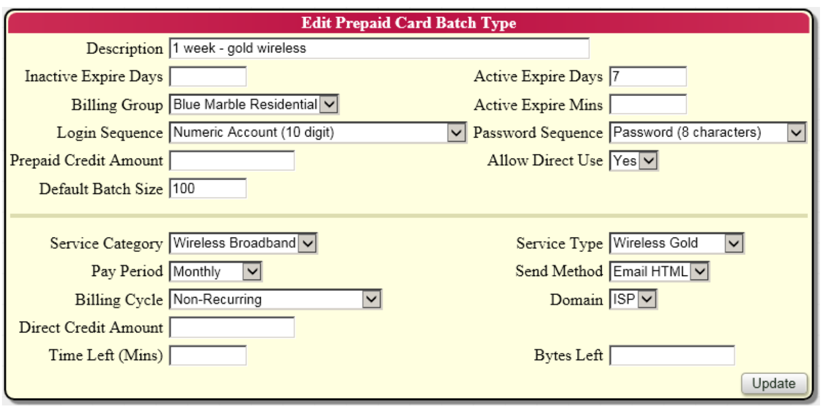
Field	Description
Description	Text describing the type and purpose of the sequence
Login Use	When "Yes" sequence is intended for use to generate the card login field. It is recommended on a per-sequence basis login or password is selected but not both.
Password Use	When "Yes" sequence is intended for use to generate the card password field. It is

	recommended on a per-sequence basis login or password is selected but not both.
JavaScript Header	This is generally used to define JavaScript functions that will be called from the JavaScript field. An example of this is a credit card format number generator.
JavaScript Field	This JavaScript code is executed once for each card generated in a prepaid batch. See "Script Parameters" in the sequence editor for more information on available helper variables.

Prepaid Batch Types

Batch types act as profiles storing configuration necessary for prepaid batch runs such that similar batches can be easily generated in the future. At least one batch type must be created before a prepaid batch can be generated.

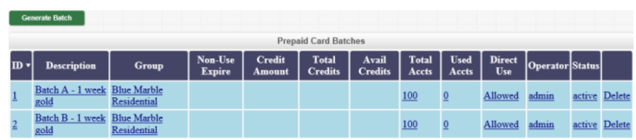




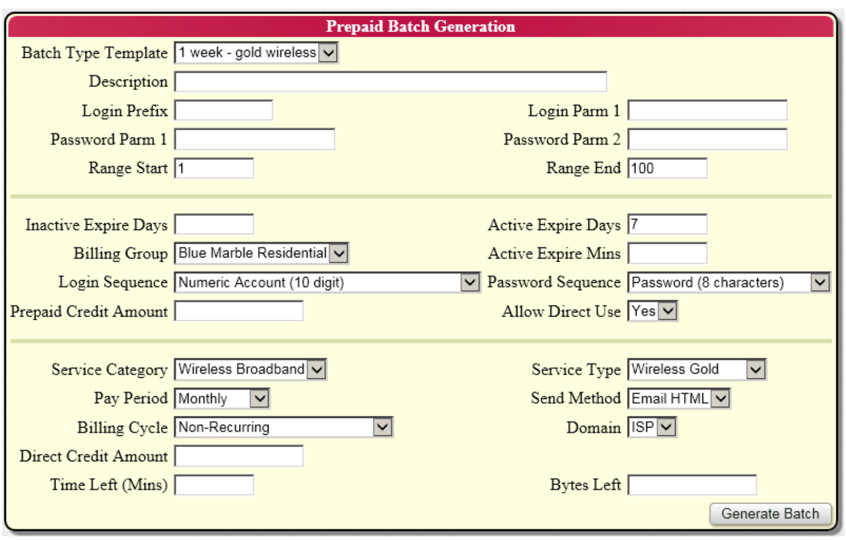
Field	Description
Description	Text describing the purpose and use of the batch type
Inactive Expire Days	Controls the "Shelf Life" of a prepaid card. When set any cards that have not been activated before "Inactive Expire Days" of the prepaid batch creation are disabled and no longer useable.
Active Expire Days	For "Direct Use" accounts set the expiration date of the account after its creation. When the pre-paid card is not used as a direct use card the Active expire days field is ignored.
Login Sequence	"Sequence" used to generate the "Card Login" fields of a pre-paid batch.
Password Sequence	"Sequence" used to generate the "Card Password" fields of a pre-paid batch.
Prepaid Credit Amount	Amount available when using the prepaid card to make payments against an existing account or when using the prepaid card through the Emerald signup server to create a new account. Note that after any amount is taken from a prepaid card it is no longer possible to use the prepaid card for "Direct Use". Similarly when a prepaid card is used as a "Direct Use" card the Prepaid Credit Amount is not available. To provide a credit amount to "Direct Use" accounts see the "Direct Credit Amount" field below.
Allow Direct Use	When enabled "Direct Use" of the prepaid card is allowed. Direct use is the ability to authenticate via RADIUS using the cards login and password to gain network access without having to take any further steps such as going through a "Sign-Up" process.
Default Batch Size	By default the number of prepaid cards to be generated per pre-paid batch run. NOTE: As with most options default batch size can be overridden during the creation of a

	prepaid batch.
Billing Group	Billing Groups serve two purposes. First when a prepaid card is used for "Direct Use" this determines which billing group the new "Direct Use" MBR will be associated with. Second, billing group restricts non-"Direct Use" uses of the pre-paid card to accounts which share the same Organization as the selected billing group.
Service Category	Applies to "Direct Use" accounts only. Service Category of new Direct Use account.
Service Type	Applies to "Direct Use" accounts only. Service Type of new Direct Use account.
Pay Period	Applies to "Direct Use" accounts only. Pay Period of new Direct Use account.
Send Method	Applies to "Direct Use" accounts only. Send Method of new Direct Use account.
Billing Cycle	Applies to "Direct Use" accounts only. Billing Cycle of new Direct Use account.
Domain	Applies to "Direct Use" accounts only. Domain of new Direct Use account.
Time Left	Applies to "Direct Use" accounts only. Time Left of new Direct Use account.
Bytes Left	Applies to "Direct Use" accounts only. Data remaining of new Direct Use account.
Direct Credit Amount	Applies to "Direct Use" accounts only. Available balance of new Direct Use account.

Prepaid Batches



The prepaid batch menu allows the creation of new prepaid batches by clicking the "Generate Batch" button under prepaid batches. Additionally all previously created card batches are available from this menu as well as usage statistics of each batch. By clicking on an existing batch all prepaid cards in that batch and the status of each are displayed.



Field	Description
Batch Type Template	Choose a prepaid batch type to be used as a template for generating the prepaid batch.
Description	Text uniquely illustrating the purpose of the new prepaid batch.
Login Prefix	Static prefix prepend to the card login field of all prepaid cards generated in this batch
Login Parm 1	Optional parameter reserved for custom purpose.
Password Parm 1	Optional parameter reserved for custom purpose.

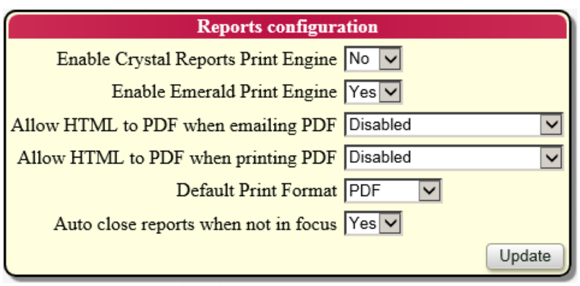
Password Parm 2	Optional parameter reserved for custom purpose.
Range Start	Starting number used for prepaid batch generation
Range End	Ending number used for prepaid batch generation. Number of prepaid cards created in the batch is equal to "Range End" minus "Range Start"
***	See Prepaid Batch Types above for descriptions of the remaining options in prepaid batches.

REPORTS & LOGS

This menu provides for the configuration of the Emerald reporting system and log management.

Settings

Provides system wide configuration to specify which print engines are installed and useable as well as engine specific configuration options.



Field	Description
Enable Crystal Reports Print Engine	Enables the use of the Crystal reports for report rendering. Enabling this option requires crystal reports runtime to be properly installed. Before enabling this setting run "crprint" from CLI within Emerald folder. Command line parameter usage information should be returned. If an error such as missing crpe32.dll is displayed please check installation of crystal and environment path to resolve any problems prior to enabling crystal report engine.
Enable Emerald Print Engine	Enables use of Emerald for report rendering. Recommended this setting always remain enabled.
Allow HTML to PDF when emailing PDF	When reports such as Invoices & Statements are emailed to customers having requested PDF formatted version of report and report renderer does not support direct output to PDF enabling this setting causes HTML rendered reports to be converted to PDF. If requested output format is not PDF or report renderer is able to directly output as PDF then no conversion is performed and this setting

<table>
<tr><td></td><td>is ignored.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Disabled</td><td>HTML rendered reports shall not be converted to PDF.</td></tr>
<tr><td>Convert using wkhtmltopdf</td><td>Converts HTML reports to PDF using "wkhtmltopdf" software available for Windows and Linux from https://wkhtmltopdf.org

Executable "wkhtmltopdf" must be installed and accessible from operating system search path by Emerald prior to enabling this setting. If wkhtmltopdf is inaccessible or PDF processing fails reports automatically fallback to HTML rendering.

Note for Linux users accurate rendering of PDF documents require locally installed fonts. If rendered output appears with oversized fonts that run off the page or display with poor quality vs similar HTML display in browser install more fonts on the Emerald server to improve rendering quality.

Note for Windows users if system PATH environment variable is changed system must be rebooted before processes launched as windows services from service control manager recognize updated PATH information.</td></tr>
</table></td></tr>
<tr><td>Allow HTML to PDF when printing PDF</td><td>When reports are printed from Emerald client, operator default print format is PDF and report renderer does not support direct output to PDF enabling this setting causes HTML rendered reports to be converted to PDF.

If requested output format is not PDF or report renderer is able to directly output as PDF then no conversion is performed and this setting is ignored.

It is recommended this setting always remain 'Disabled' for best rendering quality and performance.

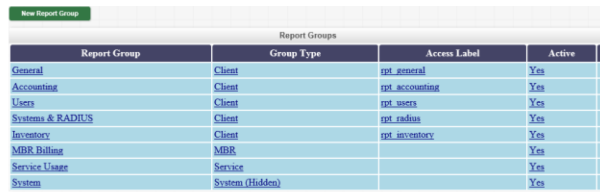
See option table for "Allow HTML to PDF when emailing PDF" above for additional information relevant to this configuration.</td></tr>
<tr><td>Default Print Format</td><td>Default format to be used when rendering reports for printing. Reports using Emerald report templates are always rendered in HTML format. If crystal reports are used PDF format is also available. If the selected print format is not available for given reporting technology the best available format is selected automatically. Operator print format preference overrides this setting.</td></tr>
<tr><td>Auto close reports when not in focus</td><td>When "Yes" once the report loses focus and is no longer in the foreground the report window is automatically closed. When "No" the report remains open in the background window.

It is recommended this option remain enabled to prevent users from forgetting about report windows in the background and having new</td></tr>
</table>

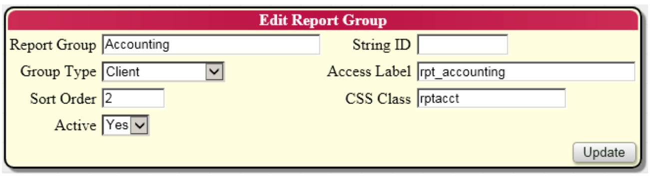
	reports display in background windows hidden from view.

Report Groups

Report groups act as container for related reports. Examples of report groups include "General", "Accounting" and "Users". Each report group is able to control where in the Emerald client reports are presented as well as any access control requirements for operator access.



Report Group	Group Type	Access Label	Active
General	Client	rpt_general	Yes
Accounting	Client	rpt_accounting	Yes
Users	Client	rpt_users	Yes
Systems & RADIUS	Client	rpt_radius	Yes
Inventory	Client	rpt_inventory	Yes
MBR Billing	MBR		Yes
Service Usage	Service		Yes
System	System (Hidden)		Yes



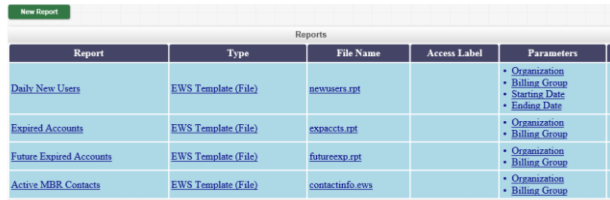
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Report Group</td><td>Unique label describing the report group. When group type is "Client" name of the group is displayed in the Reports menu of Emerald client.</td></tr>
<tr><td>String ID</td><td>See Common fields</td></tr>
<tr><td>Group Type</td><td>Defines where reports assigned to this report group are displayed within the Emerald client.

<table>
<tr><th>Group Type</th><th>Description</th></tr>
<tr><td>Client</td><td>Reports in this group are displayed from the main Emerald client / Reports menu.</td></tr>
<tr><td>MBR</td><td>Reports in this group are MBR centric accessible only from MBR level Reports menu.</td></tr>
<tr><td>Service</td><td>Reports in this group are Service centric accessible only from Service level Reports menu.</td></tr>
<tr><td>System (Hidden)</td><td>Members of this group generally represent reports called by Emerald system which do not appear in specific reporting menus. This includes reports used for rendering invoices, statements and payment receipts.</td></tr>
</table></td></tr>
<tr><td>Access Label</td><td>Access label associated with a security object group controlling operator access to this report group.

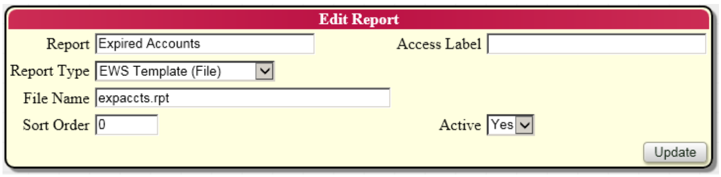
For example the "Accounting" report group has an access label "rpt_accounting". This label is assigned to object group 'Reports - Accounting' enabling any operator with access to this group to run reports associated with the group.

By default access label is applied to all reports within the report group unless an access label is set at the report level in which case access label of the report overrides the report group label.</td></tr>
<tr><td>Sort Order</td><td>Determines order report groups appear within Emerald client / Reports menu in ascending order. If multiple groups have the same sort order group name is used as a secondary sort.</td></tr>
<tr><td>CSS Class</td><td>CSS class for group specific styling</td></tr>
<tr><td>Active</td><td>When "Yes" the report group is available to be displayed within Emerald client.</td></tr>
</table>

Reports

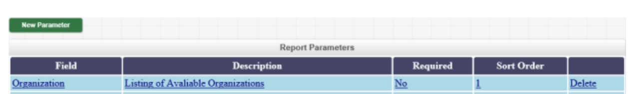


Once a report group is defined one or more reports can be added to the group. Custom reports developed by your organization may be added from this menu. It is recommended those interested in developing custom reports use existing reports located in the Emerald/web/reports folder as an example or template for designing custom reports. Before customizing existing reports please make a copy with a different filename and make changes to the copy. Avoid making changes to included report files directly as all changes are automatically overwritten as Emerald maintenance updates are installed.

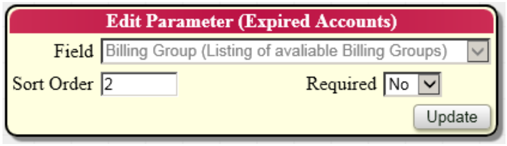


Field	Description
Report	Enter an identifying description of the Report. This description will be used within the 'Report' selection pick lists throughout Emerald.
Access Label	Configuring an access label at report level overrides report group level access label requirement.
Report Type	Report type determines whether report will be defined by a report file or SQL Query. **Report Type** / **Description** EWS Template (File): Report is either a ews report template or crystal report located in the Emerald\web\reports folder. When developing custom reports using Emerald templates please contact support for technical documentation detailing template language. Reports designed using Emerald templates require knowledge of HTML, SQL and Emerald database schema. Quick Report (SQL Query): Report is a quick report defined by SQL Query. While more limited in terms of presentation options every quick report offer display and data export in popular formats including XML, CSV and Excel.
File Name	Enter the actual filename of the report. This file should be located in the emerald report folder. The file extension of the report may be left as .rpt even when the actual report file is an Emerald report having a ews file extension. This allows for the same report definition to use either Emerald for report rendering or a third party reporting system such as crystal reports depending on which reporting engines are enabled and the format requested by the operator when printing the report.
Sort Order	See Common fields
Active	When "Yes" this report is displayed with other reports within the report group. When "No" the report is hidden from view and prevented from being run.

REPORT PARAMETERS



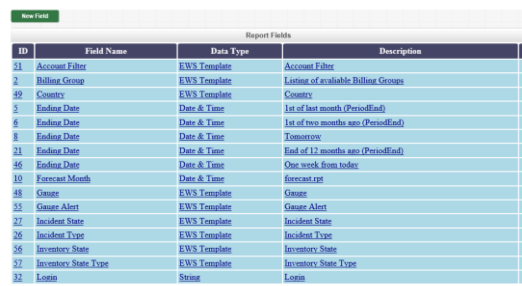
Once a report has been added to a report group you may assign any parameters supported by the report to filter relevant output. Parameters are presented to the operator as input fields just prior to executing the report. Typical examples of parameters include Organization, Billing Group, Region, Market Tag and date ranges. Parameters usable by a report are specific to each report.



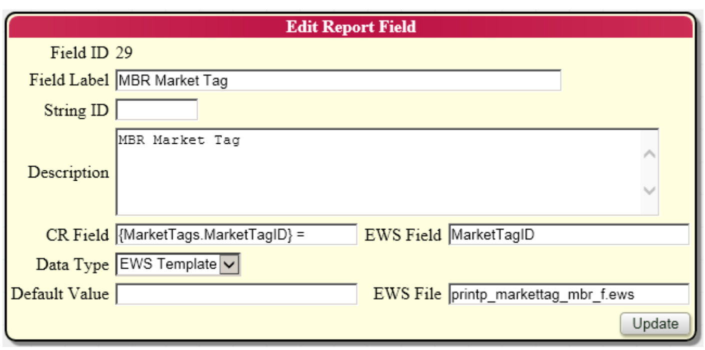
Field	Description
Field	Selection of appropriate parameter field configured from report fields menu below.
Sort Order	Determines sequence parameter fields are displayed to the operator in ascending order
Required	A report parameter marked required must have a value entered before that report can be run. Most report parameters are optional.

Report Fields

When running a custom report it may be necessary to prompt the operator to answer various questions so the report displays data relevant to the operators query. For example a report that shows all call records for a period of time may ask for starting and ending dates to show the call information as well as restricting the call record display to a subset of accounts based on region, billing group, organization or other criteria. To accomplish this report fields are configured through report field editor shown below. Once report field is created it is available to be assigned to any report that has been configured to accept the new field.



ID	Field Name	Data Type	Description
51	Account Filter	EWS Template	Account Filter
2	Billing Group	EWS Template	Listing of avaliable Billing Groups
49	Country	EWS Template	Country
5	Ending Date	Date & Time	1st of last month (PeriodEnd)
6	Ending Date	Date & Time	1st of two months ago (PeriodEnd)
8	Ending Date	Date & Time	Tomorrow
21	Ending Date	Date & Time	End of 12 months ago (PeriodEnd)
46	Ending Date	Date & Time	One week from today
10	Forecast Month	Date & Time	forecast.rpt
48	Gauge	EWS Template	Gauge
55	Gauge Alert	EWS Template	Gauge Alert
27	Incident State	EWS Template	Incident State
26	Incident Type	EWS Template	Incident Type
56	Inventory State	EWS Template	Inventory State
57	Inventory State Type	EWS Template	Inventory State Type
32	Login	String	Login



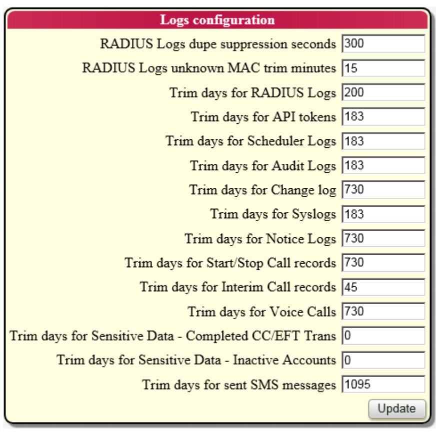
Field	Description
Field ID	Unique number representing this field. When adding a new report field ID must be larger than 10000 to prevent any conflict or chance of your field being overwritten by future software updates. All ID fields 10000 and below are reserved for IEA Software use only.
Field Label	Field name to display to the operator
String ID	See Common fields
Description	Text describing the use of this field and optionally default value
CR Field	Crystal reports field name
EWS Field	Emerald report field name accessible to report templates via "Variables" table.

<table>
<tr><td>Data Type</td><td>Data type defines input field format and validation

<table>
<tr><th>Data Type</th><th>Description</th></tr>
<tr><td>Numeric</td><td>Data entered must conform to a numeric value</td></tr>
<tr><td>String</td><td>Data entered can contain alphanumeric characters</td></tr>
<tr><td>Date & Time</td><td>Data entered is a date or date and time field formatted per operator date preference.</td></tr>
<tr><td>EWS Template</td><td>Data field display based on EWS template file. See Emerald Web Extensions guide for information on creating ews template files.</td></tr>
</table>
</td></tr>
<tr><td>Default Value</td><td>Default value of this data field</td></tr>
<tr><td>EWS File</td><td>When Data Type is "EWS Template" this represents the ews template name to use.</td></tr>
</table>

Log Trimming

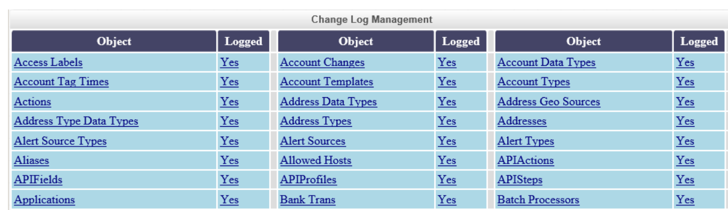
The Logs Global option provides configuration for maximum number of days in which to store log and other data within the system. Trimmed records are permanently deleted from the system.



Field	Description
RADIUS Logs dupe suppression seconds	When multiple RADIUS authentication failures are logged for the same user + failure cause within the specified window of time all duplicate log entries are removed. Frequency at which log deduplication occurs is controlled by scheduled task "Trim and deduplicate RADIUS logs" with a default run interval of 30 minutes.
RADIUS Logs unknown MAC trim minutes	When RADIUS authentication failure occurs due to an unknown login and username is a MAC address trim can be performed more rapidly after set number of minutes to better manage log entries caused by MAC based authorization systems. Recommended default value is 15 minutes.
Trim days for RADIUS Logs	Number of days to keep RADIUS authentication failure logs searchable from Emerald Client / Reports / RADIUS Log.
Trim days for API tokens	Number of days to keep transaction tokens created via Emerald API. All tokens older than set number of days are removed regardless of status.
Trim days for Scheduler Logs	Logs detailing to the successful or unsuccessful completion of scheduled tasks as searchable from Emerald Admin / Scheduler / Search Task History.
Trim days for Audit Logs	Days to retain audit log searchable from Emerald Client / Reports / Audit Logs. Audit logs include details on some changes and errors such as login failures and denied access.
Trim days for Change log	Days to retain detailed data change history searchable from Emerald Client / Reports / Change History.

Trim days for Syslogs	Maximum upper limit on the number of days to retain Syslog messages regardless of syslog source or type dependent expiration.
Trim days for Notice Logs	Days to retain logs of emails sent or failed from the notification system as searchable from Emerald Client / Reports / Mail Logs
Trim days for Start/Stop Call records	Days to retain call detail records from RADIUS accounting. Minimum retention period may be required by local and national law in some areas. It is recommended trim days be set no lower than 45 days.
Trim days for Interim Call records	Days to retain interim call accounting data. If Call usage rating is enabled this should be set no lower than 45 days otherwise there is no recommended minimum.
Trim days for Voice Calls	Days to retain call detail records imported into the VoiceCalls table.
Trim days for Sensitive Data - Completed CC/EFT Trans	Days after completed CC/EFT transaction to remove account numbers from the transaction database. If configured account numbers related to approved transactions less than 180 days old are retained regardless of the setting to allow credits against previous transactions to succeed. If blank or 0 trimming is disabled.
Trim days for Sensitive Data - Inactive Accounts	Days after MBR or Service inactivation to remove sensitive information from accounts including passwords and credit card and banking account numbers. If blank or 0 trimming is disabled.
Trim days for sent SMS messages	Days to retain queued SMS messages as searchable from Emerald Client / Reports / SMS Logs

Change Logging



Change Log Management

Object	Logged	Object	Logged	Object	Logged
Access Labels	Yes	Account Changes	Yes	Account Data Types	Yes
Account Tag Times	Yes	Account Templates	Yes	Account Types	Yes
Actions	Yes	Address Data Types	Yes	Address Geo Sources	Yes
Address Type Data Types	Yes	Address Types	Yes	Addresses	Yes
Alert Source Types	Yes	Alert Sources	Yes	Alert Types	Yes
Aliases	Yes	Allowed Hosts	Yes	APIActions	Yes
APIFields	Yes	APIProfiles	Yes	APISteps	Yes
Applications	Yes	Bank Trans	Yes	Batch Processors	Yes

Details of operator account and configuration changes throughout much of Emerald are recorded to the change log. Once recorded change data is searchable from Emerald Client / Reports / Change History. Data logged includes added or removed records, when modified column level details of prior and new values, change date, operator or customer responsible for change and network address. Change logging is always performed within same transactions as underlying changes to ensure reliable logging of covered events.

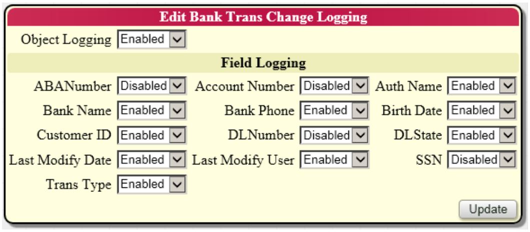
Several important limitations apply to change logging. Logging is not available for a small number of account and configuration tables. Logging does not cover any of the following: Change to Emerald database outside of Emerald, executing SQL queries or processes which create or change data directly. For example creation of invoices by Emerald billing engine does not cause log entries to be created for creation of invoices and invoice line items however when an operator manually creates an invoice and line items using the POS invoice feature this data is logged.

Change logging may be enabled or disabled at table and column levels to provide operators some flexibility to manage type and volume of stored log data. By default change logging is disabled for table and fields which contain sensitive account information such as passwords and account numbers. Log retention period is configured via Log Trimming menu described above.

In order for operators to search change history the following access requirements must be met.

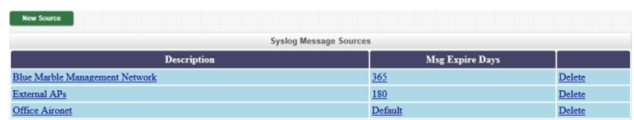
- Operator must have object group access to ' Reports - Change History' or be a global administrator

- Operator must have global group access to all MBRs
- Operator must have read access corresponding with specific tables they are viewing within the change log



Field	Description
Object Logging	When "Enabled" logging of changes related to the entire object or table are performed subject to any field level restrictions. When "Disabled" no change log of any changes to object or table are recorded.
Data Fields ***	When "Enabled" field level detail associated with add or change event may be logged for this field. When "Disabled" no add or change related data associated with the field is logged.

Syslog Sources

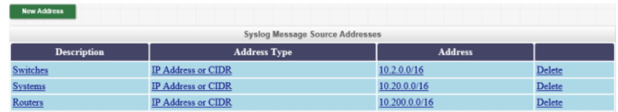


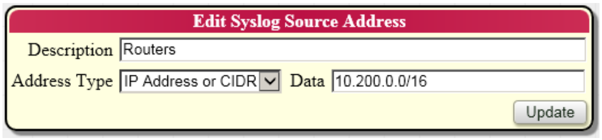
Syslog sources enable incoming syslog messages to be classified by their source. Once a source is defined one or more IP addresses or networks are assigned to classify incoming syslog messages by source address. Currently in the case multiple syslog sources are defined and two or more sources match source address of an incoming syslog message one of the sources is selected at random rather than selection by most specific match.

Field	Description
Syslog Source	Unique label describing the message source
Sort Order	See Common fields
Message Expiration (Days)	If set retention period of syslog messages matched to this source is limited to configured number of days. If not set or if expiration days are more than "Trim days for Syslogs" Log Trimming setting then syslog retention period is determined by log trimming. If expiration days is set 0 then any syslog message matching this source will be discarded and not transmitted to Emerald.

Source Addresses

Once a syslog source is created one or more source networks can be assigned. IPv4 and IPv6 IP addresses as well as IPv4/v6 subnets in CIDR form are accepted.

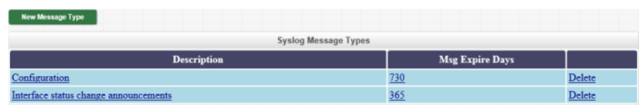




Field	Description
Description	Description of IP or Network
Address Type	Reserved for future use
Data	IPv4/IPv6 Address or subnet in CIDR form

Syslog Msg Types

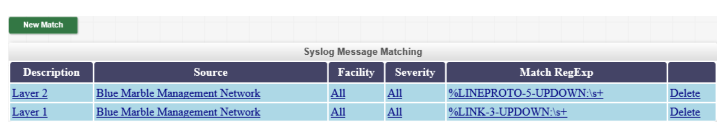
Syslog message types enable incoming syslog messages to be classified by their content. Once a message type is defined one or matching expressions are assigned to classify incoming syslog message type.

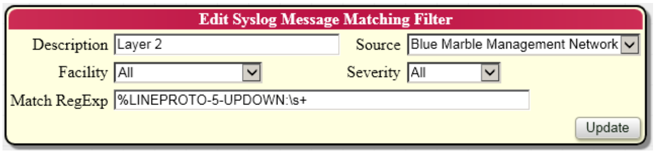


Field	Description
Description	Unique label describing the message type
Sort Order	See Common fields
Message Expiration (Days)	If set retention period of syslog messages matched to this message type is limited to configured number of days. If not set or if expiration days are more than "Trim days for Syslogs" Log Trimming setting then syslog retention period is determined by log trimming. If expiration days is set 0 then any syslog message matching this message type will be discarded and not transmitted to Emerald.

Message Matching Expressions

Once a message type is created one or more matching expressions can be assigned. If any matching expression of message type completely matches the expressions criteria then message is assigned to that message type.

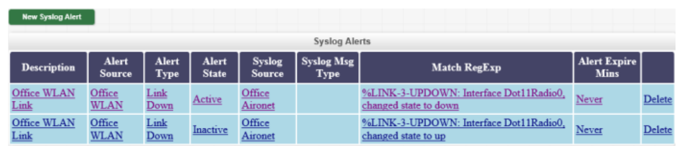


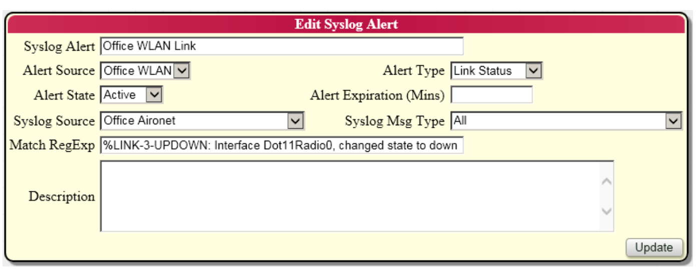


Field	Description
Description	Unique label describing the match expression
Source	If configured message source be of selected syslog source to match
Facility	If configured message must have matching syslog facility to match
Severity	If configured message must have matching syslog severity to match
Match RegExp	If configured message must satisfy the Perl compatible regular expression. The design and troubleshooting of regular expressions is not supported.

Syslog Alerts

Syslog alerts enable incoming syslog messages to activate or inactivate alerts in real-time. Syslog alerts tie together syslog and alerting system specific settings to classify incoming syslog messages and trigger appropriate alert defined as alert source + alert type.

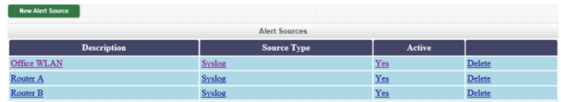


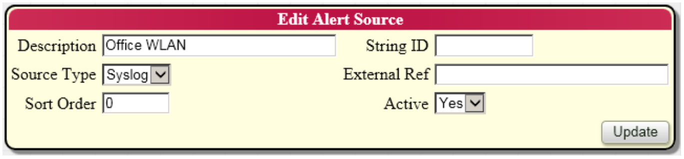


Field	Description
Syslog Alert	Description of alert often based on elements of Alert Source + Alert Type + Alert State.
Alert Source	Specific location/system/subject this alert is referencing. See Alert Sources
Alert Type	Reason for the alert. See Alert Types
Alert State	When "Active" the alert condition for alert source + alert type is being triggered. When "Inactive" the active alert is being cleared.
Alert Expiration (Mins)	Optionally causes an active alert to be cleared automatically if active for more than configured minutes.
Syslog Source	If set syslog message must be from this syslog source.
Syslog Msg Type	If set the syslog message must match selected syslog message type.
Match RegExp	Perl compatible regular expression to match against syslog message needed to change this alerts state. Design and troubleshooting of regular expressions is not supported.
Description	Additional information describing purpose of this alert.

Alert Sources

Alert sources can represent general classes of systems or specific instances of systems, subsystems and locations depending on the context of the alert.

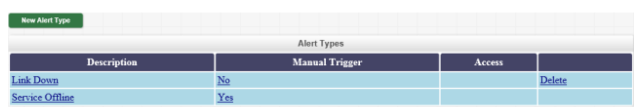




Field	Description
Description	For global alerts not raised for specific MBRs or services description represents unique label fully qualifying target of the alert. For example if an alert relates to overall status of a router the unique name of that router is entered. If an alert relates to specific subsystems of a router such as a network interface both the unique name of the router and subsystems should be included with the label. When alerts will be raised at the MBR or service level alert sources generally reflect a type of system, subsystem or technology rather than specific instances.
String ID	See Common fields
Source Type	Represents the information source used to trigger or reset alerts. Each available source type will provide its own interface to alerts. Currently the only supported source type is Syslog configured from Syslog Alerts menu.
External Ref	See Common fields
Sort Order	See Common fields
Active	When "Yes" any raised alerts using this source type are visible. When "No" alerts even if currently triggered are not visible and no notifications related to events from this source are transmitted.

Alert Types

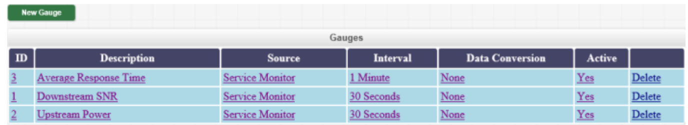
Alert type indicates the reason for an alert. Examples of alert types include "Link Down", "Low Storage" and "Poor Signal".



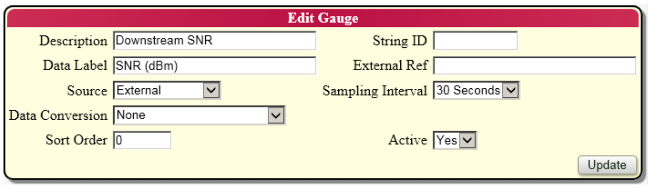
Field	Description
Alert Type	Unique description of reason for an alert
String ID	See Common fields
Manual Trigger	When "Yes" operators are able to manually activate and inactivate alerts of this type.
Access Label	See Common fields
External Ref	See Common fields

Gauges

Service quality metrics such as signal, bandwidth, latency, error rate and packet loss can be stored with each service account and reviewed from gauge graph in Emerald Client / MBR / Service / Reports menu. Thresholds automatically alert operators of any potential problems when viewing "show service" menu based on current real-time data. Data is used to identify potential service quality problems and transmit notifications as problems are noticed.



ID	Description	Source	Interval	Data Conversion	Active	
3	Average Response Time	Service Monitor	1 Minute	None	Yes	Delete
1	Downstream SNR	Service Monitor	30 Seconds	None	Yes	Delete
2	Upstream Power	Service Monitor	30 Seconds	None	Yes	Delete



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Unique label detailing what information is to be reported with this gauge</td></tr>
<tr><td>String ID</td><td>See Common fields</td></tr>
<tr><td>Data Label</td><td>Data label is informational text appears in legend of chart when viewing line graphs of data associated with this gauge. Label normally includes brief description and y-axis unit of measure of chart. If left empty default value of 'Data' is displayed within chart legend.</td></tr>
<tr><td>External Ref</td><td>See Common fields</td></tr>
<tr><td>Source</td><td>Selects method to be used for data collection. Currently the only available method is "External" which requires calling GaugeAdd procedure described below.</td></tr>
<tr><td>Sampling Interval</td><td>Represents expected interval at which new data is to be collected for each Gauge + Service. The sampling interval is also used to infer dwell time of any alerts defined for the gauge.</td></tr>
<tr><td>Data Conversion</td><td>Provides for automatic conversion of collected data into other forms.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>None</td><td>No data conversion is performed. Data is assumed to be in form suitable for presentation as a gauge value.</td></tr>
<tr><td>Counter to units per second</td><td>Converts monotonically increasing counter information such as count of errors or packets into averaged per-second rate.

Should new data be recorded with a value lower than previously recorded value it is assumed to be result of counter reset to zero.</td></tr>
<tr><td>Counter to units per minute</td><td>Converts monotonically increasing counter information such as count of errors or packets into averaged per-minute rate.

Should new data be recorded with a value lower than previously recorded value it is assumed to be result of counter reset to zero.</td></tr>
<tr><td>Counter to units per hour</td><td>Converts monotonically increasing counter information such as count of errors or packets into averaged per-hour rate.

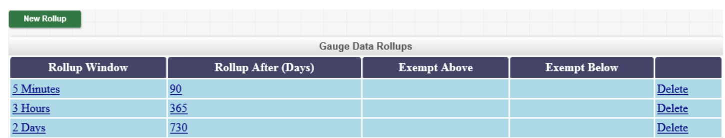
Should new data be recorded with a value lower than previously recorded value it is assumed to be result of counter reset to zero.</td></tr>
</table></td></tr>
<tr><td>Color</td><td>Determines line color when gauge is charted on a graph. Any valid CSS color name (e.g. blue, red, green. Etc) or hex RGB (e.g. #55ff88) value is supported. When left blank a line color is automatically selected.</td></tr>
<tr><td>Sort Order</td><td>See Common fields</td></tr>
<tr><td>Active</td><td>Inactivates the gauge. For automatic sources deactivation normally halts data collection associated with that gauge.</td></tr>
</table>

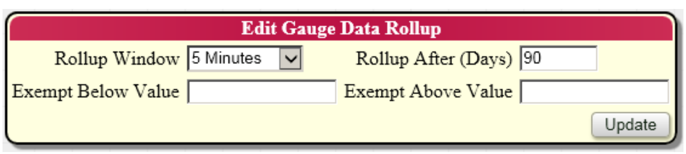
At this time service monitoring interface is available to facilitate automatic customer account level collection. External data can be collected by calling gauge_add action within Emerald API or by calling the stored procedure "GaugeAdd" with following parameters:

Parameter	Description
GaugeID	ID field corresponding with the desired gauge from list of gauges displayed in this configuration menu.
AccountID	Account ID of the service gauge data is being recorded for
StartDate	Time of the event or data sample
Data	Floating point value corresponding with event or data sample. It is recommended data be sourced by averaging a number of samples within sampling interval of the gauge.

Gauge Data Rollups

Rollups reduce amount of gauge data stored over time by averaging existing data into fewer less detailed records as data ages. Exceptions can be set to prevent rollup if data value is above or below a certain value keeping important information from being lost due to averaging during rollup. Any number of rollups is allowed by gauge to enable gradual reduction of storage requirements over time.

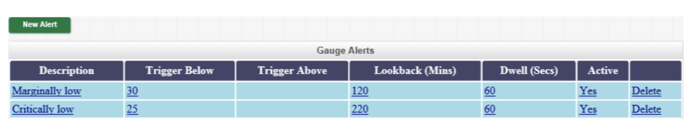


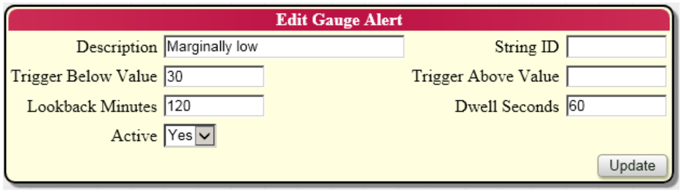


Field	Description
Rollup Window	New desired level of detail after data has been rolled up.
Rollup After (Days)	Age in days of data after which to trigger rollup.
Exempt Below Value	When data has a lower value than what is configured here rollup is not performed.
Exempt Above Value	When data has a higher value than what is configured here rollup is not performed.

Gauge Alerts

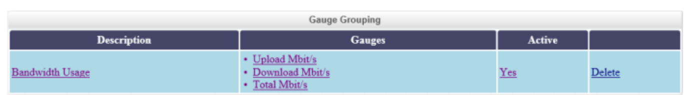
Gauge alerts are shown with service level gauge graph, "show service" menu and other gauge reports and notices. When recorded gauge data falls above or below a given threshold operators are alerted to any potential service affecting problems.



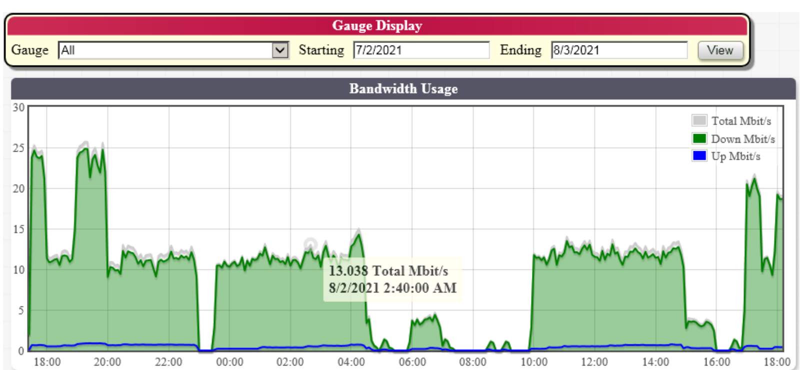


Field	Description
Description	Alert description is shown in gauge graph, service level alerts and related reports and notices.
String ID	See [Common fields](#)
Trigger Below Value	Indicates alert can be activated if data is below this value
Trigger Above Value	Indicates alert can be activated if data is above this value
Lookback Minutes	How far back in minutes to look for data that can trigger the alert. Increasing lookback increase overhead required when determining state of this alert.
Dwell Seconds	Number of seconds (based on gauge sampling interval and number of samples) this threshold must persist within the lookback period before the alert is activated.
Active	When "Yes" alert is available to be displayed to the operator. When "No" this alert is not processed or displayed.

Manage Grouping



Grouping enables sets of gauges with data in common units to be organized into a single chart rather than displayed separately. For example if gauge data is collected on customer bandwidth usage for upload, download and combined total rate rather than three separate charts for each direction (down, up, total) grouping enables all three data points to be combined into a single chart.

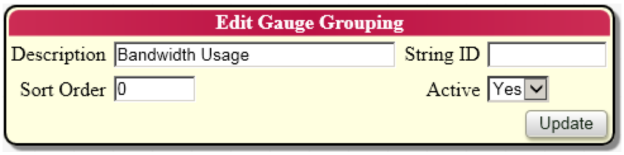


Once gauge grouping has been configured the choice to organize gauges into groups in the service gauge report is based on the following criteria:

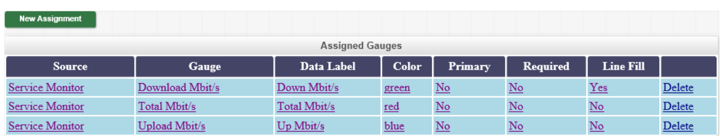
- Data for all gauges marked as required within the gauge group must be present
- Data for two or more gauges of the gauge group is available and have not been previously assigned to a different gauge group.

- Gauge groups matching the highest number of gauges are preferred over gauge groups matching a lower number of gauges having available data. If there is a tie the gauge group with the lowest sort order followed by the oldest defined gauge group is used.

If multiple gauge groups are chosen to organize related data and there are overlapping gauges between groups then data for the same gauge will be displayed within each grouped chart. Any remaining gauges not assigned to one or more gauge groups is displayed normally as an ungrouped chart.



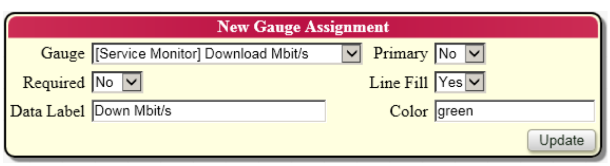
Field	Description
Description	Appears in the title area of the gauge chart detailing type of data being presented
String ID	See [Common fields](#)
Sort Order	Controls order grouped charts appear in the service gauge reporting menu and also services as a secondary tie breaking in the event available service gauge data matches multiple overlapping groupings.
Active	When "Yes" grouping is enabled. When "No" grouping is not performed in the service gauge reporting and related charts are either distributed to another gauge group or displayed as separate ungrouped charts.


New Assignment

Assigned Gauges

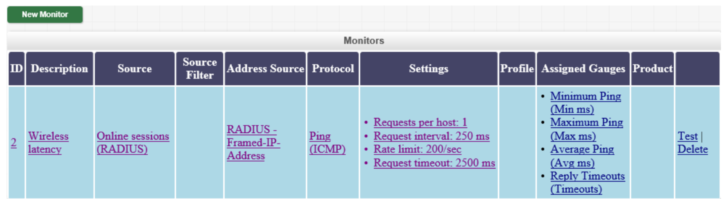
Source	Gauge	Data Label	Color	Primary	Required	Line Fill	
Service Monitor	Download Mbit/s	Down Mbit/s	green	No	No	Yes	Delete
Service Monitor	Total Mbit/s	Total Mbit/s	red	No	No	No	Delete
Service Monitor	Upload Mbit/s	Up Mbit/s	blue	No	No	No	Delete

Once the gauge group is defined two or more gauges should be assigned to the group. All gauges within a gauge group should share a common set of units. For example a gauge reporting bandwidth data rate should not be combined with a gauge reporting signal noise levels.



Field	Description
Gauge	Gauge to be assigned to the group
Primary	When "Yes" any alert trigger levels assigned to this gauge are displayed in the grouped chart.
Required	When "Yes" the gauge must be present in the services gauge data in order for this group to be selected.
Line Fill	When "Yes" the area below the line graph displayed in the chart is shaded. When "No" only the line is rendered without area shading.
Data Label	Data label is informational text appears in legend of chart when viewing line graphs of data associated with this gauge. Label normally includes brief description and y-axis unit of measure of chart. If left empty any gauge level data label is used by default. Each gauge within a gauge group should have a unique data label.
Color	Determines line color when gauge is charted within the group. Any valid CSS color name (e.g. blue, red, green. Etc.) or hex RGB (e.g. #55ff88) value is supported. When left blank the gauges default color is used.

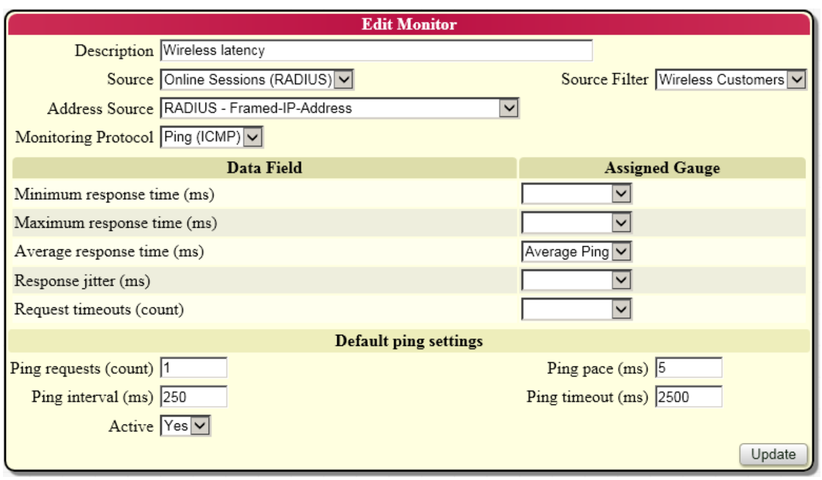
Service Monitoring



Service monitoring offers collection of NetFlow / IPFIX, Ping and SNMP data from customer connections to assist in troubleshooting and quality assurance. All data collected is recorded to one or more gauges as assigned within this menu and subsequently available for review within service level reporting menu of MBRs as well as used to provide threshold alerts to operators as configured within gauge.

Prior to configuring service monitoring following prerequisite configuration steps are required for Ping and SNMP monitoring. For flow based monitoring see the Emerald Network Collector documentation.

1. Enable service monitoring scheduled task to periodically collect service monitoring data. From Emerald Admin / Scheduler / Configure Schedules edit and set active "Process service monitoring" task.
2. Gauges must be configured with a source of "Service Monitor" for each desired data point you wish to collect using service monitoring.
3. Optionally any needed Service Filters necessary to restrict service monitoring to desired subset of accounts.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Description</td><td>Summary outlining purpose of this monitor. Summary should generally include the type of data collected and accounts to be monitored.</td></tr>
<tr><td>Source</td><td>Determines the source of accounts and related parameters for service monitoring such as hosts and SNMP settings necessary for data collection.

<table>
<tr><th>Source</th><th>Description</th></tr>
<tr><td>Online sessions (RADIUS)</td><td>Services to be monitored are based on listing of currently active and authorized sessions as provided by RADIUS accounting data.

When this source is selected "Address Source" field below is used to choose how host information for monitoring is obtained.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Service assigned inventory</td><td>Services to be monitored are based on equipment from inventory assigned to Emerald services.

When this source is selected "Assigned Product" and related fields determine assigned product and sourcing of host information for monitoring.</td></tr>
<tr><td>Service custom data</td><td>Services monitored are based on presence of service level custom data fields.

For flow monitoring data field "NetFlow IP Range" (ID: 11) is required.

For Ping monitoring data field "Ping IP" (ID:31) is required.

For SNMP the following service data fields are available:
SNMP IP (ID:26)
SNMP Login (ID:27)
SNMP Password (ID:28)
SNMP Priv Password (ID:29)
SNMP Community (ID:30)
Any defaults covering data fields above configured within this service monitoring are overridden by presence of service custom data fields.

Required fields depend on SNMP version selected and associated SNMP security setting. If any required fields are unavailable then affected services are ignored and shall not be included for monitoring.</td></tr>
</table>
</td></tr>
<tr><td>Source Filter</td><td>Optional service filter used to restrict applicability of service monitoring to a subset of eligible accounts based on the selected Source above.

For example to restrict service monitoring to subset of RADIUS authenticated sessions using wireless access technology then source field above is set "Online Sessions" and source filter configured to include only service types related to wireless access.</td></tr>
<tr><td>Address Source</td><td>When source is "Online sessions" service host address for monitoring is determined by selecting one of the following options.

<table>
<tr><th>Source</th><th>Description</th></tr>
<tr><td>RADIUS - Framed-IPv6-Address, Framed-IP-Address</td><td>Framed-IPv6-Address from RADIUS accounting is preferred falling back to Framed-IP-Address when not present.</td></tr>
<tr><td>RADIUS - Framed-IP-Address, Framed-IPv6-Address</td><td>Framed-IP-Address from RADIUS accounting is preferred falling back to Framed-IPv6-Address when not present.</td></tr>
<tr><td>RADIUS - Framed-IPv6-Address</td><td>Framed-IPv6-Address from RADIUS accounting. When attribute not present the associated service is not monitored.</td></tr>
<tr><td>RADIUS - Framed-IP-Address</td><td>Framed-IP-Address from RADIUS accounting. When attribute not present the associated service is not monitored.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>RADIUS - NAS-Identifier</td><td>NAS-Identifier field from RADIUS accounting. When attribute not present the associated service is not monitored. The NAS-Identifier field is derived from one of the following ordered attributes: NAS-IPv6-Address, NAS-IP-Address, NAS-Identifier.</td></tr>
<tr><td>Service Assigned Inventory</td><td>When selected host information for monitoring is based on item level data associated with service assigned inventory. When selected "Assigned Product" field below is required.</td></tr>
<tr><td>Service Custom Data</td><td>When selected host information for monitoring is based on service custom data associated with service account of a currently online service. See "Source / Service Custom Data" above for details on the custom data fields.</td></tr>
</table>
</td></tr>
<tr><td>Assigned Product</td><td>Determines inventory product associated with service assigned inventory items for purposes of defining host information for monitoring.

This field is only visible when Source field above is set "Serviced Assigned Inventory" or "Online Sessions" where Address Source field is subsequently set "Service Assigned Inventory".</td></tr>
<tr><td>Product Address Source</td><td>Source of host address information for Ping / SNMP monitoring within inventory item level attributes of "Assigned Product" field above.</td></tr>
<tr><td>Product Community Source</td><td>Source of SNMP community information for SNMP v1 and v2c monitoring within inventory item level attributes of "Assigned Product" field above. Community may alternately be sourced from default community configured below or service level SNMP Community custom data field.</td></tr>
<tr><td>Product Privacy Password Source</td><td>Source of SNMP privacy password information for SNMP v3 monitoring within inventory item level attributes of "Assigned Product" field above. Privacy password may alternately be sourced from default privacy password configured below or service level "SNMP Priv Password" custom data field.</td></tr>
<tr><td>Product Username Source</td><td>Source of SNMP username information for SNMP v3 monitoring within inventory item level attributes of "Assigned Product" field above. Username may alternately be sourced from default SNMP Username configured below or service level "SNMP Login" custom data field.</td></tr>
<tr><td>Product Password Source</td><td>Source of SNMP password information for SNMP v3 monitoring within inventory item level attributes of "Assigned Product" field above. Password may alternately be sourced from default SNMP Password configured below or service level "SNMP Password" custom data field.</td></tr>
<tr><td>Monitoring Protocol</td><td>Means of data collection for service monitoring.

<table>
<tr><th>Protocol</th><th>Description</th></tr>
<tr><td>Ping (ICMP)</td><td>Transmit ICMP echo "ping" requests to hosts and collect response metrics.</td></tr>
<tr><td>SNMPv1</td><td>Transmit SNMPv1 queries to host and collect response data</td></tr>
<tr><td>SNMPv2c</td><td>Transmit SNMPv2c queries to host and collect response data</td></tr>
<tr><td>SNMPv3</td><td>Transmit SNMPv3 queries to host and collect response data</td></tr>
<tr><td>NetFlow / IPFIX</td><td>Receive data flows from NetFlow / IPFIX exporters via EmerNet flow collector.</td></tr>
</table>
</td></tr>
<tr><td>SNMP Profile</td><td>Selecting a profile configured via SNMP Profiles allows one or more SNMP OIDs assigned to the profile to be mapped to gauges enabling collection of relevant data fields. Typically each profile will correspond to a unique vendor/model of a device to be monitored.</td></tr>
</table>

	If new OIDs are subsequently assigned to an SNMP Profile and the profile specifies a default gauge for the new SNMP OID data for that gauge will automatically begin to be recorded by corresponding service monitor(s) unless the gauge is removed for OID within service monitor configuration.
Data Field / Assigned Gauge	For monitors using ping protocol a static set of data fields are displayed to enable data collection of chosen metrics to the assigned gauge. At least one data field should have a gauge assigned to it. For monitors using SNMP protocol both available data fields and gauge assignment defaults depend on the SNMP profile assigned to this service monitor. Availability of gauges for assignment depends on configuration of gauges from Emerald Admin / Reports & Logs / Gauges menu.
Ping requests	Number of ping requests to transmit per host. More ping requests offer better insights into jitter and packet loss at the expense of more outgoing packets.
Ping interval	When number of ping requests is greater than 1 this field determines minimum amount of time which must elapse in milliseconds since transmission of a prior request before a subsequent request can be transmitted to a given host.
Ping pace	Outgoing packets are scheduled to occur at most within regular intervals of milliseconds configured by pace setting. Increasing pace reduces network and systems impact of ping packets at the expense of bulk ping operations taking longer to complete. If multiple ping service monitors are configured and executed by the same service monitoring scheduled task then lowest pace setting across all active ping protocol service monitors is used for that execution. For examples of pacing settings please see following table:

Example	Description
5	One request per 5 milliseconds (200 requests per second)
1	One request per millisecond (1000 requests per second)
0.25	Four requests per millisecond (4000 requests per second)
0.10	Ten requests per millisecond (10000 requests per second)
10	One request per 10 milliseconds (100 requests per second)
100	One request per 100 millisecond (10 requests per second)

Ping timeout	Maximum elapsed time in milliseconds since transmission of ping packet to wait for a ping response. Any late responses received after ping timeout are ignored.
SNMP Community	Default community string to use with SNMP v1 and v2c. If specified community is used only when both service level "SNMP Community" custom data field and community mapped to an inventory item via "Product Community Source" above are unavailable. If no source of SNMP community is available then monitoring is not performed for affected services.
SNMP Username	Default Username for SNMP v3 user security. If specified Username is used only when both service level "SNMP Login" custom data field and Username mapped to an inventory item via "Product Username Source" above are unavailable. If "SNMP Auth Protocol" field is set MD5 or SHA and no source of Username is available then monitoring is not performed for affected services.
SNMP Auth Protocol	Hash algorithm to be used with SNMP v3 user security. Algorithm selected must match configuration within SNMP server or user authentication fails.
SNMP Password	Default Password for SNMP v3 user security. If specified Password is used only when both service level "SNMP Password" custom data field and Password mapped to an inventory item via "Product Password Source" above are unavailable. If "SNMP Auth Protocol" field is set MD5 or SHA and no source of Password is available then monitoring is not performed for affected services.

	A strong password of at least 16 characters is recommended.
SNMP Privacy Password	Default Privacy Password for SNMP v3. Privacy password acts as an encryption key to protect SNMP request and response packets from eavesdropping. Privacy passwords are separate from username & password for SNMP user authentication. If specified Privacy Password is used only when both service level "SNMP Priv Password" custom data field and Password mapped to an inventory item via "Product Privacy Password Source" above are unavailable. If "SNMP Privacy Protocol" field is set AES or DES and no source of Privacy Password is available then monitoring is not performed for affected services. A strong privacy password of at least 16 characters is recommended.
SNMP Privacy Protocol	Encryption algorithm to be used to encrypt SNMP v3 packets. Algorithm selected must match configuration within SNMP server or user authentication fails.
Flow Filter	Flow filters offer a means of excluding or including packets with certain characteristics from the usage data compiled by EmerNet.
Active	When "Yes" this service monitor may be included for processing by the "process service monitoring" scheduled task. When "No" monitoring is disabled.

Advanced service monitor scheduling

Typically all non-flow based service monitors run from a single "Process service monitoring" scheduled task. This is generally sufficient for periodic monitoring of up to tens of thousands of services. Those requiring periodic monitoring of significantly more services or those with geographically diverse operations seeking more localized collection points can use following information to configure customized schedules.

All monitoring activities execute from Emerald scheduler included with Emerald suite. Any number of schedulers may be installed licensing restrictions not withstanding at different locations throughout your organization as necessary provided database connectivity is available. When multiple schedulers are installed they either work collaboratively coordinating execution of scheduled tasks amongst themselves or tasks can be specifically designated to execute only on specific schedulers.

For localized collection:

- Install instance of Emerald scheduler close to area where data collection will occur
- Disable default "Process service monitoring" task.
- Create a replacement task assigned to specific scheduler using "Schedule Server" field within Configure Schedules.
- Set MonitorID=x parameter in scheduled task to restrict execution of service monitors to specific monitor. See task parameter information below for details.
- Use service filtering to restrict applicability of monitor to only local services

To scale a service monitor:

- Install additional instances of Emerald scheduler
- Disable default "Process service monitoring" task.
- For each scheduler create a replacement task specific to scheduler using "Schedule Server" field within Configure Schedules.

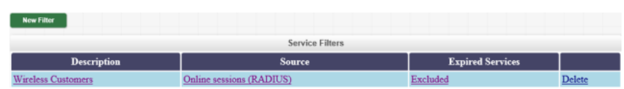
- Set DistKey=x, DistMax=y parameters as appropriate for each scheduler. See task parameter information below for details.

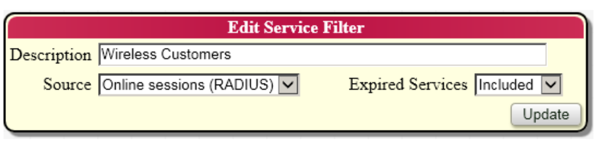
Service monitor operates by executing ews template "monproc.ews". When configuring schedules the task type is set "ews" to run ews templates. Parameter field of the task contains a series of attributes as comma separated key=value pairs. For example **file=monproc.ews, MonitorID=5** runs the service monitor with a monitor id of 5.

Parameter	Description
file	Name of ews template to execute. For service monitor this is always monproc.ews
MonitorID	Restrict execution to a specific service monitor. The MonitorID corresponds with the "ID" column displayed within the Emerald Admin / Reports & Logs / Service Monitoring. If MonitorID is not specified then all active service monitors are executed.
DistKey	DistKey and DistMax work together to distribute work to be done by service monitors across different scheduler services. This is achieved by dividing work into "DistMax" count of equal parts then assigning each part "DistKey" to individual Emerald schedulers. If DistKey or DistMax is not specified then all applicable services are processed and no distribution of work is performed. Example configuration where service monitor runs across three Emerald schedulers: • Scheduler A - parameter: **file=monproc.ews, DistKey=1,DistMax=3** • Scheduler B - parameter: **file=monproc.ews, DistKey=2,DistMax=3** • Scheduler C - parameter: **file=monproc.ews, DistKey=3,DistMax=3**
DistMax	See DistKey

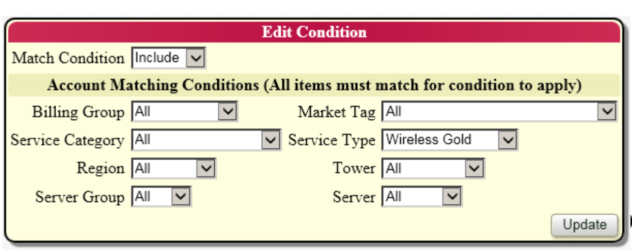
Service Filters

Filters enable service monitoring to be restricted to subsets of otherwise applicable services. Examples of service filter include restricting service monitoring to VIP customers, specific access technologies or regions.





Field	Description
Description	Label detailing unique purpose of this filter
Source	References service monitor account source. When configuring a service monitor source field must match this source field before the filter is allowed to be assignable to service monitor.
Expired Services	When "Included" active services with an expired status continue to be monitored while expired until MBR or service is inactivated. When "Excluded" services with an expired status are not monitored while remaining expired.

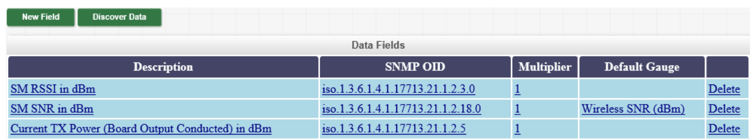


Once a service filter is configured one or more match conditions are applied to the filter. "Include" match conditions indicate while there is a complete match matching services are to be included for monitoring.

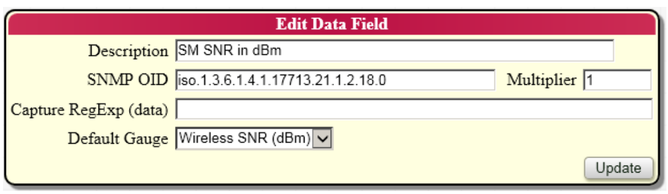
"Exclude" conditions exclude services having a complete match with the condition from monitoring. Exclude conditions takes precedence over include. If both include and Exclude conditions match then matching service shall not be included for monitoring.

If no matching conditions are assigned to a service filter or service monitor is configured without a filter then no filtering is performed and all eligible services corresponding with "source" field are included with monitoring.

SNMP Profiles



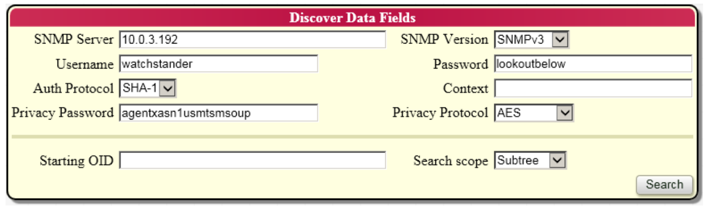
When configuring SNMP based service monitoring profiles offer menu of relevant SNMP fields for collection of gauge data. Profiles are often organized by device vendor and model allowing for collection of device specific metrics. Prior to setting up service monitoring at least one SNMP profile is necessary.



Field	Description
Description	Informational text explaining SNMP OID. Description is displayed within service monitoring interface once this SNMP profile has been selected.
SNMP OID	OID representing SNMP data field to be recorded. Either numeric OID or name may be used when corresponding MIBs are available.
Multiplier	Multiplier for numeric value of data field to be recorded. For example if SNMP value is 100 and multiplier is 2 then 200 is recorded as gauge value.
Capture RegExp	If a numeric value to be captured is embedded within a string then regular expressions can be used to extract values via PCRE named capture to "data" variable. Otherwise when collecting numeric data normally this field is left blank. When defining regular expressions it is important to constrain captured values such that only numeric data is collected. Should regular expression not be matched or no data is contained within the capture then no data is recorded to the associated gauge. For example to extract version number "32.3" from sample below: \s+Version\s+(?<data>\d+\.\d+)\s+ "Nabisco SOI Software, C350 Software (CHIP-KE9BL7-R), Version 32.3 ELF, RELEASE SOFTWARE…"
Default Gauge	When configuring service monitoring if a default gauge is selected then gauge configuration from this profile is used by default. If a service monitor is using an existing SNMP profile and a new OID is subsequently added to the profile having a default gauge then service monitor will automatically begin collecting data associated with new OID unless the new gauge is manually removed within service monitor

	configuration.

Discover Data



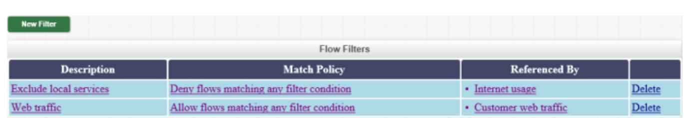
Within an SNMP Profile Discover feature works by connecting to a SNMP server, "walking" servers supported MIB tree to produce a menu of all available data fields. Items from the list are then easily selected for inclusion in a corresponding SNMP profile. It is recommended community string or username for discover have full read access to all data fields to offer a complete set of data fields for selection.

If a loop is detected during "walk" process all SNMP OID information retrieved prior to occurrence of loop are displayed normally but no information after loop is included. Depending on size of servers MIB tree and network round trip latency it may take some time for walk operation to complete and display search results.

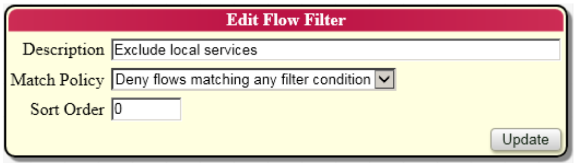
Field	Description
** SNMP connection	Select appropriate SNMP version and enter standard SNMP connection details to establish connection to SNMP server.
Starting OID	Position within servers MIB tree to begin retrieving data. Normally to retrieve all available data fields Starting OID is left blank and scope set "Subtree" This can be used to restrict a search to a specific SNMP "table". Enter OID corresponding to base of table and select One-level from the search scope field. Starting OID can also be used to work around presence of a loop during "walk" process by resetting the starting place to a point in the MIB tree after occurrence of loop.
Search scope	When "Subtree" all OIDs within the server MIB from the position of starting OID forward are retrieved. When "One-level" only OIDs on the same level of MIB hierarchy are retrieved.

Once search completes click "Add to profile" to the right of one or more OIDs you wish to incorporate into the SNMP profile. It is recommended when finished click "Return to Profile" and set descriptions detailing purpose of each OID added to the profile.

Flow Filters



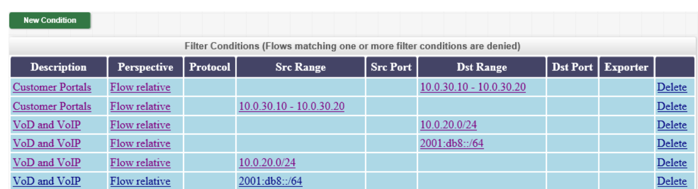
When configuring service monitors using the NetFlow / IPFIX monitoring protocol flow filters provide a means of excluding or including packets with certain characteristics from usage data compiled by EmerNet. Example of flow filters include charting bandwidth usage by protocol or separating locally provided services such as VoD and VoIP from external network usage.



Field	Description
Description	Filter description is displayed in filter selection list when configuring service monitors using NetFlow / IPFIX monitoring protocol.
Match Policy	Determines outcome of matching one or more filter conditions. **Policy** — **Description** Deny flows matching any filter condition — Flows are allowed by default except when one or more conditions of the flow filter are matched. Allow flows matching any filter condition — Flows are disallowed by default except when one or more conditions of the flow filter are matched.
Sort Order	See Common fields

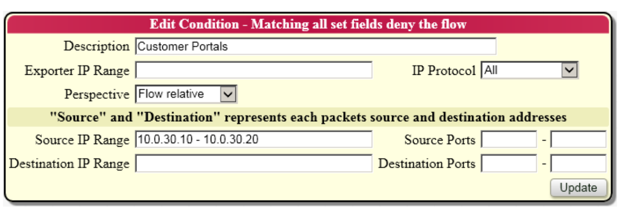
Filter Conditions

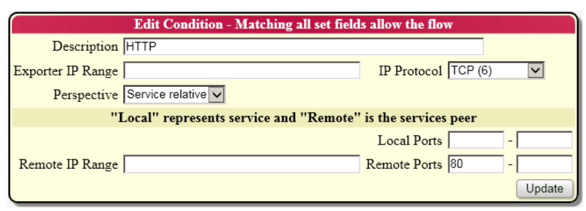
In order for a condition of a flow filter to match all filled in fields must match the flow. When there are multiple conditions only one of the conditions within the filter has to be match in order for its matching policy to apply to the flow.


New Condition

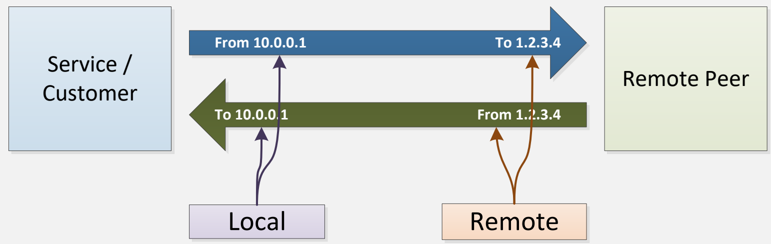
Filter Conditions (Flows matching one or more filter conditions are denied)

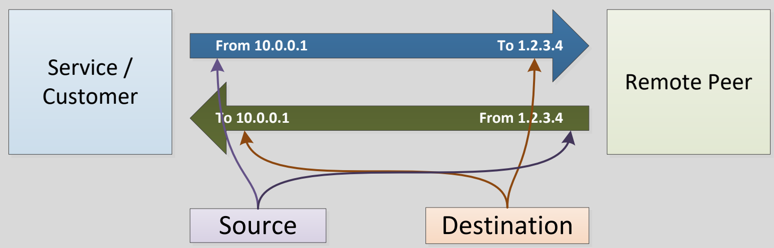
Description	Perspective	Protocol	Src Range	Src Port	Dst Range	Dst Port	Exporter	
Customer Portals	Flow relative				10.0.30.10 - 10.0.30.20			Delete
Customer Portals	Flow relative		10.0.30.10 - 10.0.30.20					Delete
VoD and VoIP	Flow relative				10.0.20.0/24			Delete
VoD and VoIP	Flow relative				2001:db8::/64			Delete
VoD and VoIP	Flow relative		10.0.20.0/24					Delete
VoD and VoIP	Flow relative		2001:db8::/64					Delete





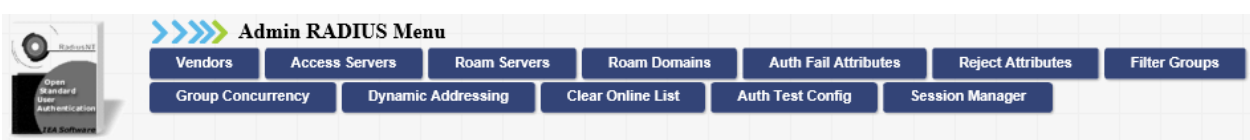
Field	Description
Description	Short summary of purpose or target.
Exporter IP Range	IP address or address range of flow exporter(s) transmitting flow records to EmerNet collector to match. Exporter IP address is viewed from the perspective of source address of NetFlow / IPFIX packets as viewed by EmerNet.
IP Protocol	IP protocol associated with a flow such as TCP or UDP.
Perspective	Manages how flows are matched to simplify configuration of filter conditions. **Perspective** — **Description**

<table>
<tr><td rowspan="2"></td><td>Service relative</td><td>Flows are viewed from the vantage point of the service regardless of flow direction.


Service relative conditions benefit from enabling a single match condition to cover flows both to and from the service.</td></tr>
<tr><td>Flow relative</td><td>Flows are viewed from the vantage point of each packets source and destination address.

</td></tr>
<tr><td>Source IP Range</td><td colspan="2">Match IP address or address range of the flows source address</td></tr>
<tr><td>Source Ports</td><td colspan="2">Match flows source port or port range</td></tr>
<tr><td>Destination IP Range</td><td colspan="2">Match IP address or address range of the flows destination address</td></tr>
<tr><td>Destination Ports</td><td colspan="2">Match flows destination port or port range</td></tr>
<tr><td>Local Ports</td><td colspan="2">Matches service port or port range in both incoming and outgoing flows</td></tr>
<tr><td>Remote IP Range</td><td colspan="2">Match service peers IP address or address range in both incoming and outgoing flows</td></tr>
<tr><td>Remote Port</td><td colspan="2">Match service peers port or port range in both incoming and outgoing flows</td></tr>
</table>

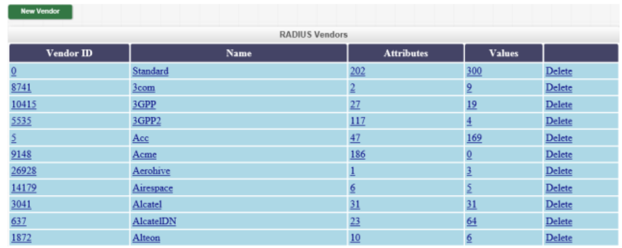
RADIUS

RadiusNT/X bundled with Emerald suite is centrally managed from this menu. In addition some local configuration may be required from within the RadiusNT/X Administrator of each local RadiusNT/X server to enable or disable features, manage TLS certificates for authentication, configure accounting queue and customize RADIUS listener addresses and ports. Please see RadiusNT/X User's guide for details on accessing and using RadiusNT/X Administrator.



Vendors (Vendor Attributes)

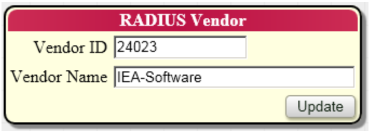
Vendor Attributes (VSAs) are a set of RADIUS attributes and values that provide unique functionality specific to product offerings of individual vendors. Support for most vendors is already included with Emerald. Additional vendors and associated attributes may be manually configured. Alternately IEA support can provide an automated update script to add any missing attributes when a vendor supplied RADIUS "dictionary" file containing vendor specific attributes is available.



New Vendor

RADIUS Vendors

Vendor ID	Name	Attributes	Values	
0	Standard	202	300	Delete
8741	3com	2	9	Delete
10415	3GPP	27	19	Delete
5535	3GPP2	117	4	Delete
5	Acc	47	169	Delete
9148	Acme	186	0	Delete
26928	Aerohive	1	3	Delete
14179	Airespace	6	5	Delete
3041	Alcatel	31	31	Delete
637	AlcatelDN	23	64	Delete
1872	Alteon	10	6	Delete

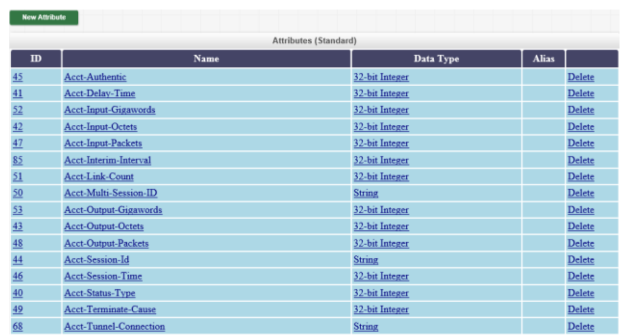


Please consult your NAS documentation for more information about supported attributes of your access hardware.

Field	Description
Vendor ID	Enter the IANA enterprise number for this Vendor. Vendor ID numbers are standard and should be supplied within your NAS documentation.
Vendor Name	Enter descriptive name of the RADIUS Vendor.

Vendor Attributes

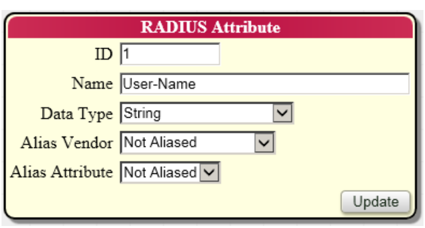
Attributes specific to each vendor are managed by selecting vendor whose attributes you would like to view or change from the vendor list.



New Attribute

Attributes (Standard)

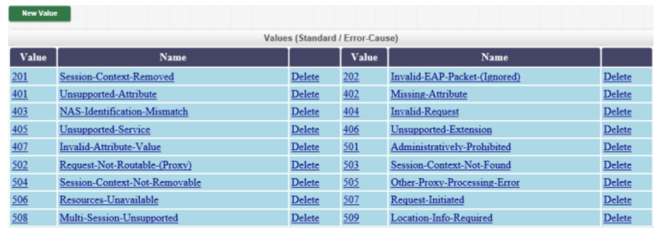
ID	Name	Data Type	Alias	
45	Acct-Authentic	32-bit Integer		Delete
41	Acct-Delay-Time	32-bit Integer		Delete
52	Acct-Input-Gigawords	32-bit Integer		Delete
42	Acct-Input-Octets	32-bit Integer		Delete
47	Acct-Input-Packets	32-bit Integer		Delete
85	Acct-Interim-Interval	32-bit Integer		Delete
51	Acct-Link-Count	32-bit Integer		Delete
50	Acct-Multi-Session-ID	String		Delete
53	Acct-Output-Gigawords	32-bit Integer		Delete
43	Acct-Output-Octets	32-bit Integer		Delete
48	Acct-Output-Packets	32-bit Integer		Delete
44	Acct-Session-Id	String		Delete
46	Acct-Session-Time	32-bit Integer		Delete
40	Acct-Status-Type	32-bit Integer		Delete
49	Acct-Terminate-Cause	32-bit Integer		Delete
68	Acct-Tunnel-Connection	String		Delete



Field	Description
ID	Enter the Attribute ID value. Please check with your NAS documentation for information on entering the correct value.
Name	Enter the appropriate Attribute name. Please check with your NAS documentation for information on entering the correct value.
Data Type	Select the appropriate type from the selections offered in the pick list. Please check with your NAS documentation for information on entering the correct value.
Alias Attribute Alias Vendor	Alias fields are used by RADIUS when recording accounting data to the Calls table to impersonate a selected attribute. This feature allows redundant attributes across vendors to be represented with a single column in the Calls table when multiple vendors provide equivalent data using their own unique VSAs. See the RadiusNT/X documentation for more information on alias attribute functionality.

Vendor Attribute Values

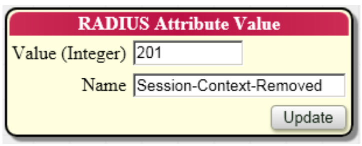
Some attributes of integer type have numeric values representing a selection list of specific predetermined meanings. For example a hypothetical attribute named "Answer" has two possible values 1 or 0. Value 1 represents "Yes" and value 0 is "No". In this case once the attribute is defined two values are added to the attribute representing 1=Yes and 0=No.



New Value

Values (Standard / Error-Cause)

Value	Name		Value	Name	
201	Session-Context-Removed	Delete	202	Invalid-EAP-Packet-(Ignored)	Delete
401	Unsupported-Attribute	Delete	402	Missing-Attribute	Delete
403	NAS-Identification-Mismatch	Delete	404	Invalid-Request	Delete
405	Unsupported-Service	Delete	406	Unsupported-Extension	Delete
407	Invalid-Attribute-Value	Delete	501	Administratively-Prohibited	Delete
502	Request-Not-Routable-(Proxy)	Delete	503	Session-Context-Not-Found	Delete
504	Session-Context-Not-Removable	Delete	505	Other-Proxy-Processing-Error	Delete
506	Resources-Unavailable	Delete	507	Request-Initiated	Delete
508	Multi-Session-Unsupported	Delete	509	Location-Info-Required	Delete



Field	Description
Value	Enter the numeric value to represent configuration option. Please check with your NAS documentation for information on entering the correct value.
Name	Enter the appropriate label describing value above. Please check with your NAS documentation for information on entering the correct value.

Access Servers (RADIUS Clients)

RADIUS clients are defined within access servers menu. Configuring IP Address and shared secret of each client is necessary before RadiusNT/X is able to accept incoming RADIUS Authentication and Accounting requests.

New Server Group

Access Server Groups

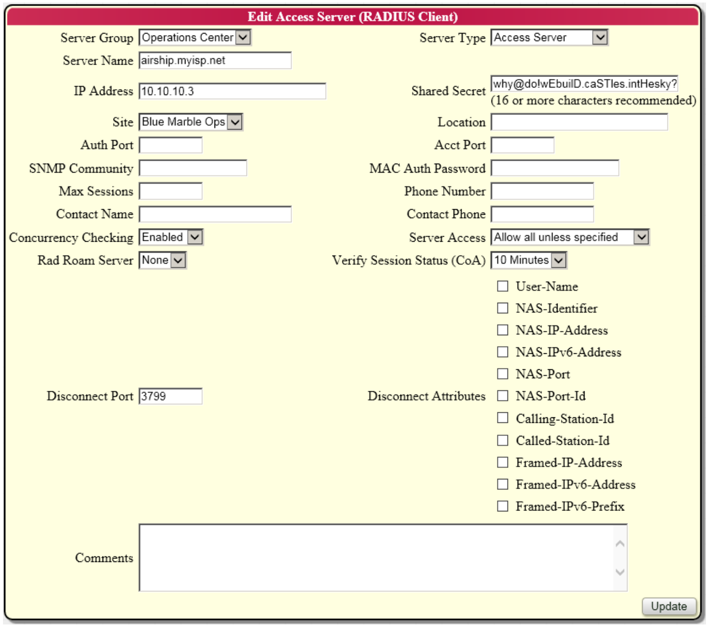
Server Group	Servers
Operations Center	[trolley.myisp.net] [carriage.myisp.net] [airship.myisp.net] [train.myisp.net] [chariot.myisp.net] [canoe.myisp.net]
Other	[localhost] [macaroni.myisp.net] [tulsa.myisp.net]

New RADIUS Client

Access Servers (RADIUS Clients)

Server	IP Address	Type	Location	Sessions	Dynamic Auth	Verify Sessions	Concurrency	Server Access	MAC Auth	
airship.myisp.net	10.10.10.3	Access Server		0 active	Enabled	10 Minutes	Enabled	Allow by Default	Disabled	Delete
canoe.myisp.net	10.10.10.6	Access Server		0 active	Disabled	Disabled	Enabled	Allow by Default	Disabled	Delete
carriage.myisp.net	10.10.10.2	Access Server		0 active	Disabled	Disabled	Enabled	Allow by Default	Disabled	Delete
chariot.myisp.net	10.10.10.5	Access Server		0 active	Disabled	Disabled	Enabled	Allow by Default	Disabled	Delete
train.myisp.net	10.10.10.4	Access Server		0 active	Disabled	Disabled	Enabled	Allow by Default	Disabled	Delete
trolley.myisp.net	10.0.3.20	Access Server		0 active	Disabled	Disabled	Enabled	Allow by Default	Disabled	Delete

Server grouping is offered to better organize RADIUS clients by geography or technology. To add a RADIUS client click the desired group from server group column then add a new client.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Server Group</td><td>Select the Server Group that applies to this Server entry. The default is the currently selected Server Group.</td></tr>
<tr><td>Server Type</td><td>Server type determines purpose of this client.
<table>
<tr><th>Server Type</th><th>Description</th></tr>
<tr><td>Access Server</td><td>RADIUS client is a NAS. Incoming RADIUS user Authentication and Accounting from this client is expected.</td></tr>
<tr><td>Emerald Client</td><td>RADIUS client is an instance of Emerald Web UI if different from a RadiusNT/X server. This authorized Emerald to transmit RADIUS authentication requests for operator initiated RADIUS authentication testing within a services RADIUS menu.</td></tr>
<tr><td>RadiusNT/X Server</td><td>RADIUS client is an instance of a RadiusNT/X server. This is used to allow transmission of reconfiguration hints to all RadiusNT/X servers when an operator clicks "Apply" from InfoBar of the Emerald Admin to refresh stored configuration.

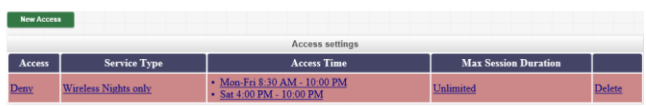
By default Emerald is distributed with a "localhost" client configured with a Server Type of RadiusNT/X server. This entry allows Emerald initiated authentication test and "Apply" reconfiguration hints when a single installation of Emerald and RadiusNT/X exist on the same server.</td></tr>
</table></td></tr>
<tr><td>Server Name</td><td>Enter an identifying name for the Server. This can be either the fully qualified domain name (FQDN) of the NAS, or just hostname of the NAS. Ideally this should match NAS-Identifier attribute transmitted by NAS.</td></tr>
<tr><td>IP Address</td><td>IP Address reflects IPv4 or IPv6 network source address of the incoming RADIUS request as viewed by the RadiusNT/X server. Please take care to consider impacts of any intervening firewalls or proxies that may rewrite source address observed by RadiusNT/X. While DNS names are also accepted use of IP address is recommended.

In the event there are multiple RADIUS clients behind a RADIUS proxy server and you would like the ability to transmit RADIUS dynamic authorization directly through to those server for use with Session manager or Online report contact information of each client may</td></tr>
</table>

	also be added as a RADIUS client even though they will not be directly transmitting RADIUS requests.
Secret	Enter the shared RADIUS secret password between RADIUS client (NAS) and RadiusNT/X. This must be exactly the same as configured on the NAS itself. A 16 or more character random shared secret containing letters, numbers and symbols is recommended.
Site	Represents physical location where this RADIUS client is located. See Sites.
Location	Server location used for informational purposes only.
Auth Port	Used only by Emerald UI when transmitting test RADIUS authentication requests or reconfiguration hints to RadiusNT/X. If defined authentication requests are transmitted to this port otherwise the default RADIUS authentication port (1812) is used. This field does not configure port RadiusNT/X servers listen for incoming RADIUS authentication requests.
Acct Port	Used only by Emerald for RADIUS accounting testing. If defined test accounting requests are transmitted to this port otherwise the default RADIUS accounting port (1813) is used. This field does not configure port RadiusNT/X servers listen on for incoming RADIUS accounting requests.
SNMP Community	Currently unused. Provided for backward compatibility.
MAC Auth Password	If MAC authentication is supported by this access server and expected to be used then MAC authentication password configured within the access server should be entered in this field exactly as configured within access server. MAC auth password is generally transmitted as the user password during MAC based RADIUS authentication.
Max Sessions	Total number of physical or logical ports the NAS is able to manage concurrently. This is used for reporting and informational purposes only.
Phone Number	The Phone Number field is used for informational purposes only.
Contact Name	Enter the name of person in charge of administering the server.
Contact Phone	Enter the phone number of the Contact person for the server.
Concurrency Checking	When "Enabled" and "(Auth) Concurrency control" is enabled in the advanced menu of RadiusNT/X administrator concurrency checking is performed for authentication requests made from this access server. When "Disabled" or "(Auth) Concurrency control" is disabled then concurrency checking is not performed during RADIUS authentication for this access server. Disabling concurrency checking also prevents Emerald session manager from counting active sessions on this server toward enforcement of concurrent login limits.
Server Access	When "(Auth) Server port access" is enabled in the advanced menu of the RadiusNT/X administrator this controls the default server access rule for this server. "Allow All Unless Specified" allows full access to all service types with RADIUS attributes and all ports unless specific deny rules have been defined. "Allow none unless specified" denies all access and requires access rules before any authentication attempts can be succeed for this access server. To configure access rules see Server Access.
Rad Roam Server	By selecting a roam server, all requests from this server will be automatically forwarded to the selected roam server and not processed locally. Use of this feature requires proxy be enabled in the RadiusNT/X administrator.
Verify Session	When not "Disabled" this feature periodically at selected interval polls sessions appearing as

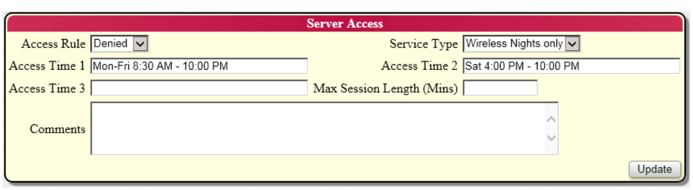
Status	active in the online report via RADIUS dynamic authorization (CoA). If session is found to no longer be active it is automatically cleared from the active session list correcting any inconsistencies in the online list caused by missing RADIUS accounting data. This feature requires Session Manager.
Disconnect Port	If this access server supports RFC3576 Disconnect or CoA messages disconnect port reflects the dynamic authorization UDP port of the access server. If disconnect port is specified Emerald will issue disconnect messages when sessions are cleared for this access server from online sessions report in "Client" / "Reports" menu. Disconnect port is also required by Session Manager.
Disconnect Attributes	In order for access servers supporting receipt of CoA/Disconnect messages to terminate active sessions this option controls which session identifying attributes are sent to the access server to identify and disconnect a unique session via the Emerald session manager or Manually via the emerald online list. Since some access devices may not accept disconnect requests with all of the attributes provides you may uncheck those attributes the access device will not accept. If you are experiencing problems with disconnect try unchecking more fields and check access server documentation for required session identifying attributes. The attribute Acct-Session-ID is always sent and cannot be disabled.
Comments	Enter any description or comment regarding the server or its configuration.

Server Access



Once an access server is defined optional server access rules can be applied. Server access controls which service types are able to authenticate from this access server as well as offering time of day, calendar and maximum session length limits.

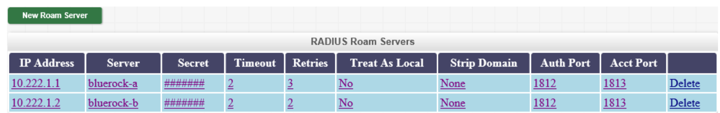
Prior to configuring server access rules please take note of the "Server Access" setting of access server. When "Allow all unless specified" access is granted globally by default and any added server access rules would generally reflect exceptions where access is explicitly denied. When "Allow none unless specified" all access is denied by default and only exceptions where access is explicitly allowed would typically be defined.



Field	Description
Access Rule	"Allowed" means access is granted when all of the criteria below is met. "Denied" means access is denied when all of the criteria below is met.
Service Type	When "All Services" the rule is not limited by service type. Otherwise the access rule is limited to selected service type.
Access Time 1,2,3	When not empty the access rule is limited to configured access times. See Common fields for detailed access time format description.
Max Session Length	Enter the maximum number of minutes that sessions matching this rule are to be limited on a per session basis only. If blank session duration is limited to 30 days by default.
Comments	Additional information or notes about this server access rule.

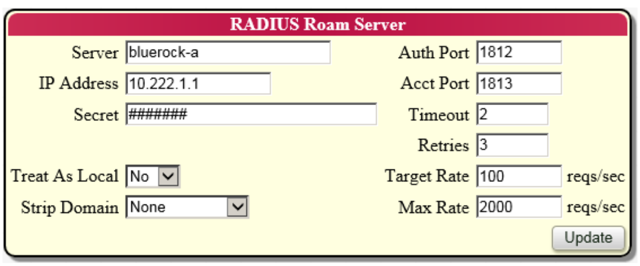
```
To use this feature "(Auth) Server port access" must also be enabled within
"Advanced" menu of RadiusNT/X administrator.  Please carefully review all
related configuration prior to enabling server access checking.
```

Roam Servers



Roam servers enable incoming RADIUS authentication and accounting from your organizations access servers to be proxied to external RADIUS servers for processing. Roam servers are typically used to operate roaming networks where subscribers of other service providers are allowed to share your organizations access network. Each roam server represents a destination RADIUS server where RADIUS requests can be proxied.

Roam servers and RADIUS proxy is not required merely to use another provider's network. For example if your customers are able to login as user@myisp to a hotspot network then the only configuration necessary is adding RADIUS client entries under for each of the providers RADIUS servers. Roaming configuration is only needed when third parties will be logging on thru your access network.



Field	Description
Server	DNS name or label of roam server
Auth Port	UDP port of destination RADIUS server to be used for RADIUS Authentication. Default authentication port is 1812.
IP Address	IPv4 or IPv6 address of the roam server RadiusNT/X is to send proxy requests.
Acct Port	UDP port of destination RADIUS server to be used for RADIUS Accounting. Default accounting port is 1813.
Secret	Enter RADIUS shared secret for the remote roam RADIUS server. This secret must exactly match shared secret configured in the roam server. It is recommended that secrets contain at least 16 characters made up of random letters, numbers and symbols.
Timeout	Number of seconds after which forwarded requests timeout if not acknowledged.
Retries	Number of times failed forwarded requests should be retried.
Treat as Local	This option indicates whether this server will be receiving requests. Select "No" in order to forward requests to the server. Select "Yes" to indicate the server is not receiving requests and Emerald should process the requests locally. This is a handy option when defining your own domains so that login attempts from specific domains will be authenticated locally rather than forwarded.

<table>
<tr><td>Target Rate</td><td>Target forwarding rate in requests per second. Used for load balancing purposes when there are several roaming servers attached to a roam domain. If there is only one roam server available Target Rate is unused.</td></tr>
<tr><td>Strip Domain</td><td>This option indicates that RadiusNT/X should remove the domain before forwarding the request. The option descriptions are as follows:

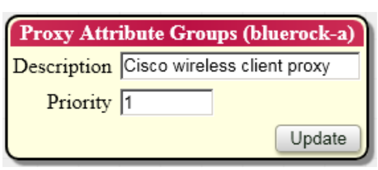
<table>
<tr><th>Strip Domain</th><th>Description</th></tr>
<tr><td>None</td><td>Domain part of the request is not stripped</td></tr>
<tr><td>Authentication</td><td>Only strip domain part from authentication requests</td></tr>
<tr><td>Accounting</td><td>Only strip domain part from accounting requests</td></tr>
<tr><td>Both</td><td>Strip domain part from authentication and accounting requests</td></tr>
</table>

Consult the system administrator of the roam server regarding the format they are expecting to receive. Normally domain is not stripped.</td></tr>
<tr><td>Max Rate</td><td>Maximum forwarding rate in requests per second. Used for load balancing purposes when there are several roaming servers attached to a roam domain. If there is only one roam server available Max Rate is unused. Max rate is not enforced when all other proxy servers in a roam domain have also exceeded their forwarding rate.</td></tr>
</table>

```
Roaming requires Authentication and or Accounting proxy to be enabled from
"Proxy" menu of RadiusNT/X administrator.  Roaming is only included with
Professional and Enterprise editions of Emerald.
```

Proxy Attribute Group

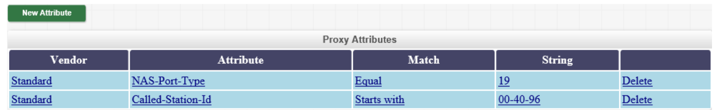
Authentication requests can be proxied based on value of a group of one or more attributes transmitted with the request. For example authentication using a specific access technology, username or MAC address can sent to an external RADIUS server for processing. Requests are proxied to the roam server when all of the attributes within an attribute group match criteria of the incoming RADIUS request.

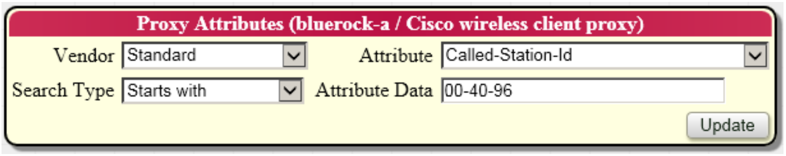


Field	Description
Description	Unique name describing criteria or purpose of this proxy attribute group.
Priority	In the event other attribute groups associated with other roam servers also match priority determines which of the roam servers is to be used. The matching group having lowest numeric value is chosen over matching groups with higher numeric values.

PROXY ATTRIBUTES

Once attribute group is created one or more attributes defining what must match in order for attribute proxy to take place are assigned to the attribute group.



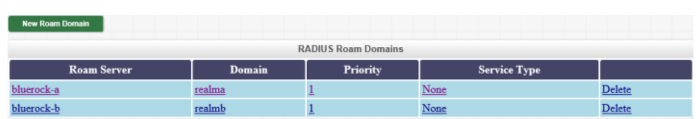


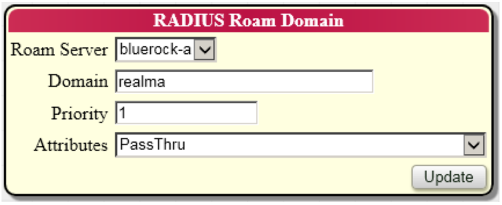
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Vendor</td><td>RADIUS vendor of corresponding attribute below</td></tr>
<tr><td>Attribute</td><td>Vendor attribute defining the attribute of RADIUS request to match</td></tr>
<tr><td>Search Type</td><td>Matching condition specifying in what way attributes value is to be matched.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>String</td><td>Exactly match string</td></tr>
<tr><td>Substring</td><td>Match any portion of a string</td></tr>
<tr><td>Equal</td><td>Exactly match integer numeric value</td></tr>
<tr><td>Less than</td><td>Is less than integer numeric value</td></tr>
<tr><td>Greater than</td><td>Is greater than integer numeric value</td></tr>
<tr><td>Ends with</td><td>Match ending portion of a string</td></tr>
<tr><td>Starts with</td><td>Match starting portion of a string</td></tr>
<tr><td>Any Value</td><td>Match anything including empty/null value.</td></tr>
<tr><td>Distributed Key</td><td>Format is "gid:gmax" where gid is group number and gmax is the total number of groups. String deterministically has approximately 1 in gmax chance of matching the distributed key.

Distributed key provides deterministic load balancing based on the contents of an attribute being matched. It is case insensitive and useful for distributing accounting information to various connection groups based on user-name or server in a way that guarantees all users or servers with the same values are always routed together to the same place.</td></tr>
<tr><td>Regular Expression</td><td>String matches Perl compatible regular expression. Documentation and support for creating regular expressions is not provided.</td></tr>
<tr><td>Not Equal</td><td>Numeric integer value is not exactly matched</td></tr>
<tr><td>Not Contains</td><td>Does not match any portion of a string</td></tr>
</table></td></tr>
<tr><td>Attribute Data</td><td>Value to search for based on attribute and search type above.</td></tr>
</table>

Roam Domains

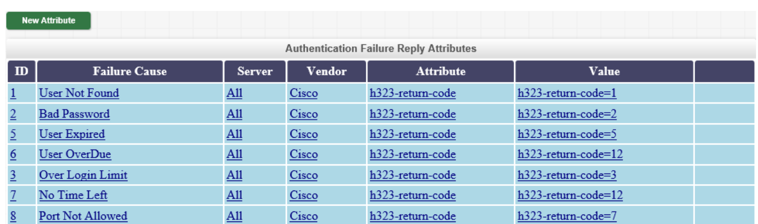
Roam domains enable outgoing proxy by match of realm name transmitted with the username of authenticating users and subsequent RADIUS accounting. This usually takes the form of users logging on as user@realm similar to an email addresses except realm name does not necessarily refer to a DNS domain.





Field	Description
Roam Server	Select the appropriate Roam Server from the pick list requests are to be proxied when there is a realm match.
Domain	Enter the realm name to be forwarded to the selected Roam Server. Enter the realm name only without the '@' symbol.
Priority	Enter the priority of the server. This is used in the case that there are duplicate entries for a particular Roam Server/Domain combination to allow for the definition of backup servers. Priorities are required to be unique per individual Roam Server/Domain. If a priority is not unique RadiusNT/X will check both servers in random order should the first return an authentication failure. Priorities with lowest numeric values take precedence over priorities with higher numeric values.
Attributes	Indicates that RadiusNT/X overrides the set of attributes the authenticating RADIUS server replied with and instead use the default set of RADIUS attributes associated to the selected Service Type. The default and recommended value is "Pass Thru" which does not alter the authentication response as it is proxied through RadiusNT/X.

Auth Fail Attributes



Authentication Failure Reply Attributes

ID	Failure Cause	Server	Vendor	Attribute	Value	
1	User Not Found	All	Cisco	h323-return-code	h323-return-code=1	
2	Bad Password	All	Cisco	h323-return-code	h323-return-code=2	
5	User Expired	All	Cisco	h323-return-code	h323-return-code=5	
6	User OverDue	All	Cisco	h323-return-code	h323-return-code=12	
3	Over Login Limit	All	Cisco	h323-return-code	h323-return-code=3	
7	No Time Left	All	Cisco	h323-return-code	h323-return-code=12	
8	Port Not Allowed	All	Cisco	h323-return-code	h323-return-code=7	

Failure reply attributes are commonly used to provide information to the end-user detailing why they were unable to login and possible actions that can be taken to address the problem. While RADIUS standard "Reply-Message" attribute generally contains text explaining cause of failure many access servers do not pass this data on to the end user and default messages may lack important details relating to how an authentication problem can be resolved.

This menu offers the option of overriding Reply-Message attribute to customized error text as well as transmitting other vendor specific attributes as supported by access servers to express more information about the cause of authentication failure. When using our Air Marshal Gateway vendor specific attribute AM-NAK-HTMLFile in IEA-Software vendor space may be used to define an error page tailored to specific failure causes such as account expiration or running out of time / data allowance.

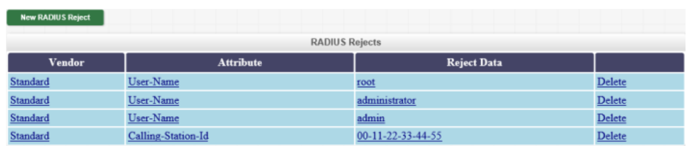
This feature differs from failure attributes configured within RADIUS service type attributes in the following important ways.

- Service type level failure attributes allow conditions that would normally lead to authentication failure to succeed with Access-Accept response rather than Access-Reject.
- This feature merely adds attributes to existing RADIUS Access-Reject response. This feature cannot be used to override RADIUS result code and transmit Access-Accept instead of Access-Reject.

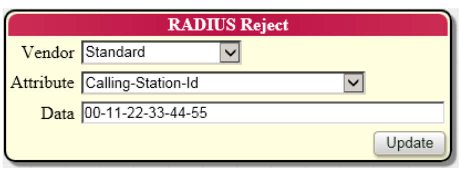
Before any configured failure attributes can be processed the Advanced menu option " (Auth) Custom auth failure attributes" within RadiusNT/X administrator must be enabled.

Field	Description
Failure Cause	Attribute defined below is only transmitted when selected authentication failure cause occurs.
Server	Restricts applicability of attribute to specified access server
RADIUS Vendor	Vendor space from which to select attribute
Attribute	Attribute to be transmitted in Access-Reject response
Attribute Value	Value of attribute to be transmitted

Rejects



The RADIUS Rejects Administrative option is used to define the sets of RADIUS attribute/value matches that RadiusNT/X will reject immediately, without actually processing the request. For instance, if you want to reject any user calling from a specific phone number, you could add an entry to the RADIUS Rejects list with the Caller-ID attribute and the specific phone number.

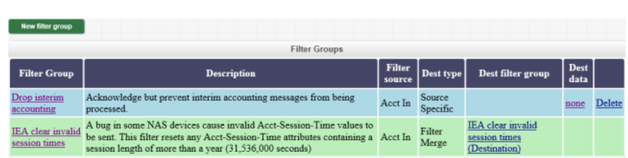


Field	Description
Vendor	Select the appropriate Vendor from the selection pick list for the desired RADIUS attribute.
Attribute	Select the appropriate Attribute from the selection pick list. Only the attributes for the above selected Vendor will be available in the pick list.
Data	Enter the Value of the attribute that is to be rejected.

```
To use this feature '(Auth) Reject attributes' must be enabled within
'Advanced' menu of RadiusNT/X administrator.
```

Filter Groups

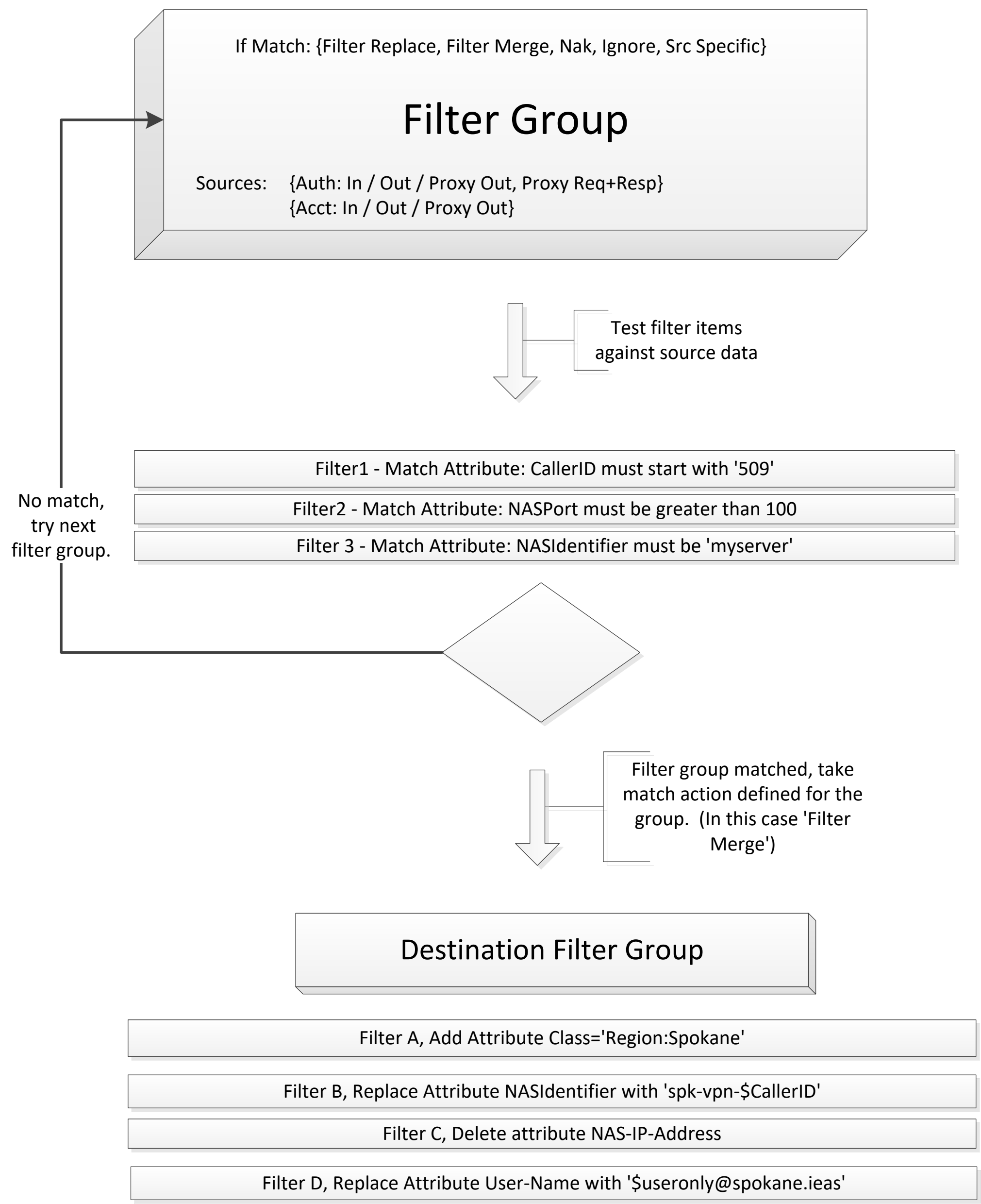
In some situations to support unique features of access servers, limit access or enforce policy in roaming



environments filter groups provides functionality to add, alter or remove attributes going in, out or passing through the server. RADIUS filtering allows the flexibility to support many unique situations. Use of filtering should be considered carefully. Applying too many filter groups can make it very difficult to understand or troubleshoot the outcome of filtering actions.

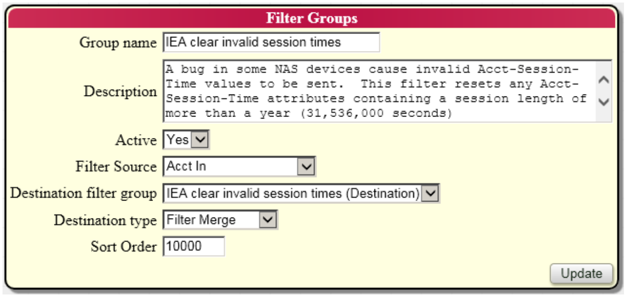
Filters have two main components. The source filter that seeks to match a criteria and the destination filter that carries out an action once a match has occurred. The diagram below shows this process in more detail.

```
Execution of attribute filters requires "Enable attribute filtering" option
in advanced section of RadiusNT/X administrator.
```



Source filter group

Source filter group defines what is to be matched based on "filter source" and what "destination group" or "destination type" is to be executed as a result of a match.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Group name</td><td>Unique description of this filter group</td></tr>
<tr><td>Description</td><td>Text describing in detail the source filter group and what conditions it is designed to match.</td></tr>
<tr><td>Active</td><td>When "Yes" this filter group is available to be matched by requests to RadiusNT/X. The "Enable attribute filtering" option in the "Advanced" menu of the RadiusNT/X admin must also be enabled.

When "No" this filter group will be ignored and not used.</td></tr>
<tr><td>Filter Source</td><td>Represents source of the data to match and also the data set to modify when processed by the destination filter group.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Destination Group</td><td>Filter is a destination filter group</td></tr>
<tr><td>Auth In</td><td>Incoming authentication requests before being processed by RadiusNT/X</td></tr>
<tr><td>Auth Req+Resp</td><td>Authentication request is used for purpose of matching source filter while authentication response is modified by destination filter.

This filter applies to successful authentication responses and does not apply in the event of authentication failure.</td></tr>
<tr><td>Auth Out</td><td>Outgoing authentication responses after being processed by RadiusNT/X.

This filter applies to successful authentication responses and does not apply in the event of authentication failure.</td></tr>
<tr><td>Auth Proxy Req+Resp</td><td>Authentication proxy request is used for purpose of matching source filter while authentication proxy response is modified by destination filter</td></tr>
<tr><td>Auth Proxy Resp</td><td>Outgoing proxy authentication RESPONSE after being processed by RadiusNT/X.</td></tr>
<tr><td>Auth Proxy Out</td><td>Outgoing proxy authentication REQUESTS after being processed by RadiusNT/X.</td></tr>
<tr><td>Acct In</td><td>Modifies incoming accounting requests before being processed by RadiusNT/X. Destination data sets an alternate local accounting table other than the default "Calls" table</td></tr>
</table>
</td></tr>
</table>

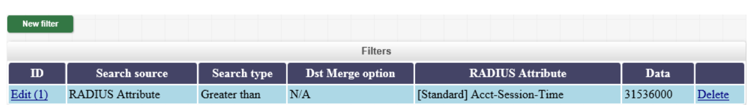
<table>
<tr><td></td><td><table><tr><td>Acct Proxy Out</td><td>Outgoing proxy accounting REQUESTS after being processed by RadiusNT/X.</td></tr></table></td></tr>
<tr><td>Destination filter group</td><td>A filter group of type "Destination Group" to process should this source filter group be matched.</td></tr>
<tr><td>Destination type</td><td>Determines how or if the destination filter group is to process RADIUS requests should the source filter group match.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Filter Replace</td><td>Removes all attributes before applying destination filter. Note certain RADIUS attributes used internally for authentication and state management are excluded from this replacement rule.</td></tr>
<tr><td>Filter Merge</td><td>Uses merge settings of individual destination filters to specify how the source attributes should be modified.</td></tr>
<tr><td>Nak</td><td>Sends an Access-Reject in response to authentication request optionally sending the "Destination Data" field as the reply-message. If Nak is used with an accounting request the request is ignored.</td></tr>
<tr><td>Ignore</td><td>Drops the request without responding. Ignore is not enforced for proxy sources.</td></tr>
<tr><td>Source Specific</td><td>Source specific is used in conjunction with "Destination Data" to specify custom behavior specific to a source.

For "Acct In" filter source destination data sets an alternate local accounting table other than the default "Calls" table.</td></tr>
</table></td></tr>
<tr><td>Sort Order</td><td>Determines order in which source filter groups are processed in order of lowest to highest sort. If multiple source filter groups have the same sort filter name is used alphabetically as a secondary sort.

Regardless of sort order authentication filter sources are processed in the order of "Auth In", "Auth Req+Resp" and "Auth Out". All input filters are processed prior to all request / response filters and finally all output filters are processed.</td></tr>
</table>

Source filters

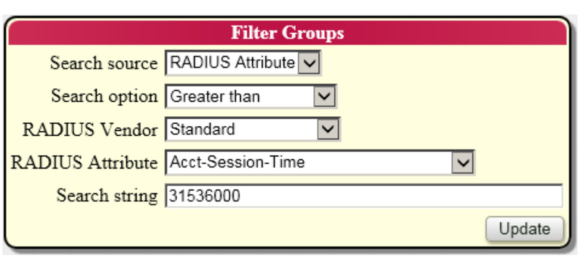

New filter

Filters

ID	Search source	Search type	Dst Merge option	RADIUS Attribute	Data	
Edit (1)	RADIUS Attribute	Greater than	N/A	[Standard] Acct-Session-Time	31536000	Delete

Once a source filter group is defined source filters are associated with new filter group to define criteria for a match of source filter group. In the example in this image we want to match source filter group to match only when accounting session duration exceeds a year.

If no source filters are defined the source filter group is executed unconditionally for each request of type "Filter Source".

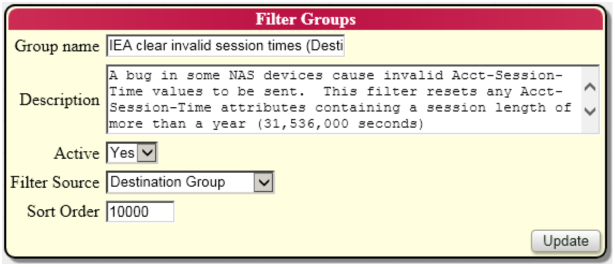


<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Search source</td><td>Determines what is to be matched.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Client IP</td><td>IP Address of the RADIUS client initiating the request</td></tr>
<tr><td>Host IP</td><td>IP Address if the RADIUS server</td></tr>
<tr><td>RADIUS Attribute</td><td>RADIUS source attribute. See "Filter Source" above.</td></tr>
<tr><td>Destination IP</td><td>IP Address of RADIUS server the request is being proxied to</td></tr>
</table></td></tr>
<tr><td>Search option</td><td>Search type specifies which match operation to use when matching RADIUS attributes. Any other "Search source" uses an exact match.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>String</td><td>Exactly match string</td></tr>
<tr><td>Substring</td><td>Match any portion of a string</td></tr>
<tr><td>Equal</td><td>Exactly match integer numeric value</td></tr>
<tr><td>Less than</td><td>Is less than integer numeric value</td></tr>
<tr><td>Greater than</td><td>Is greater than integer numeric value</td></tr>
<tr><td>Ends with</td><td>Match ending portion of a string</td></tr>
<tr><td>Starts with</td><td>Match starting portion of a string</td></tr>
<tr><td>Any Value</td><td>Match anything including empty/null value.</td></tr>
<tr><td>Distributed Key</td><td>Format is "gid:gmax" where gid is group number and gmax is the total number of groups. String deterministically has approximately 1 in gmax chance of matching the distributed key.

Distributed key provides deterministic load balancing based on the contents of an attribute being matched. It is case insensitive and useful for distributing accounting information to various connection groups based on user-name or server in a way that guarantees all users or servers with the same values are always routed together to the same place.</td></tr>
<tr><td>Regular Expression</td><td>String matches Perl compatible regular expression. Documentation and support for creating regular expressions is not provided.</td></tr>
<tr><td>Not Equal</td><td>Numeric integer value is not exactly matched</td></tr>
<tr><td>Not Contains</td><td>Does not match any portion of a string</td></tr>
</table></td></tr>
<tr><td>RADIUS Vendor</td><td>When Search source is "Radius Attribute" this reflects the RADIUS Vendor of the attribute to match.</td></tr>
<tr><td>RADIUS Attribute</td><td>When Search source is "Radius Attribute" this reflects the RADIUS Attribute to match.</td></tr>
<tr><td>Search string</td><td>Value to search for based on source/attribute and selected search option above.</td></tr>
</table>

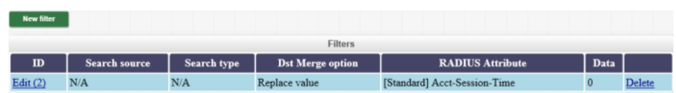
Destination filter group

The destination filter group defines what action is to be taken after "Source Filter Group" has been matched.

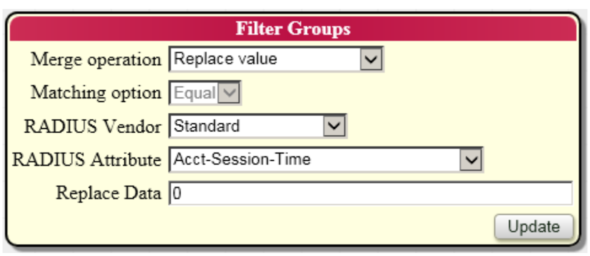


Field	Description
Group name	Unique description of this destination filter group
Description	Text describing in detail the destination filter group and what changes it has been designed to make.
Active	When "Yes" RadiusNT/X processes this destination filter. When "No" the destination filter is not processed.
Filter Source	For destination filter groups this is always "Destination Group"
Sort Order	Used for ordering of available destination filter groups in destination group selection list.

Destination filters



Once a "Destination Filter Group" is defined destination filters are responsible for carrying out the changes to RADIUS attributes prescribed for this destination filter. In example in this image the value of Acct-Session-Time is being changed to zero.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Merge operation</td><td>Determines what action is to be performed on the data.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Delete</td><td>Delete any source attribute matching the "RADIUS Vendor" and "RADIUS Attribute" fields below.</td></tr>
<tr><td>Delete matching</td><td>Delete any source attribute matching the "RADIUS Vendor" and "RADIUS Attribute" fields also having a value of "Matching Data" below.</td></tr>
<tr><td>Add</td><td>Adds a new RADIUS attribute of type "RADIUS Vendor" and "RADIUS Attribute" containing the value "New Data"</td></tr>
<tr><td>Replace value</td><td>For every RADIUS attribute matching "RADIUS Vendor" and "RADIUS Attribute" replaces its current value with the contents of the "Replace Data" field.</td></tr>
<tr><td>Add or replace value</td><td>Similar to Replace value above except that if no attributes match the attribute containing the new value is added.</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>Add attributes from query</td><td>When selected "SQL Query" field specifies a database query to retrieve attributes from authentication database then adds them to response. The result set returned by this query must contain following three columns "AttributeID", "VendorID", and "Data". If this query fails for any reason the authentication request is rejected.</td></tr><tr><td>Log query for accounting</td><td>Similar to Add attributes from query except no result set is expected and query is queued for execution into the accounting spooler. If accounting queue is full this filter operation fails. If this query fails to execute associated error is sent to the accounting log.</td></tr></table>
Match option	Used with "Delete matching" merge operation to determine search operation used to match the attribute for deletion.
RADIUS Vendor	Used with all Merge operations except "Add attributes from query" and "Log query for accounting".
RADIUS Attribute	Used with all Merge operations except "Add attributes from query" and "Log query for accounting".
Replace Data	Used with "Replace value" and "Add or replace value" merge operations. Variable reference is similar to description in SQL Query below except all reference is $attributename and the $' qualifier is not used.
New Data	Used with "Add" merge operation. Variable reference is similar to description in SQL Query below except all reference is $attributename and the $' qualifier is not used.
Matching Data	Used with "Delete matching" merge operation. Variable reference is similar to description in SQL Query below except all reference is $attributename and the $' qualifier is not used.
Connection Group	Used with "Add attributes from query" and "Log query for accounting" merge operations to specify an alternate group of ODBC connections for query execution. By default when no connection group is specified the Authentication data source is used for "Add attributes from query" and Accounting data source for "Log query for accounting" any connection groups specified must be configured in the "ODBC Connection Groups" section of the RadiusNT/X administrator. If a named connection group is not defined the query operation fails.
SQL Query	Used with "Add attributes from query" and "Log query for accounting" merge operations. In a destination filter the Data and SQL Query fields can contain variables used for setting and replacing data. All RADIUS attributes are available as variables by entering $attributename without any hyphens defined in the standard RADIUS attribute names for numeric values and $'attributename for string values using the $' variable qualifier. If qualifier is omitted any variables with non-numeric data are output as NULL. For example $'UserName contains the contents of the RADIUS User-Name attribute. This can be used to add extra data such as a realm to the start or end of the User-Name attribute as it passes through RadiusNT/X. In addition to RADIUS attributes the following special variables are available: <table><tr><th>Variable</th><th>Description</th></tr><tr><td>Useronly</td><td>Realm stripped version of RADIUS User-Name attribute</td></tr><tr><td>Accountid</td><td>Services Account ID</td></tr><tr><td>Proxystate</td><td>For proxy local proxy state used for forwarding</td></tr><tr><td>Timestamp</td><td>Current RADIUS server time in seconds / unix time</td></tr><tr><td>Serverip</td><td>IP Address of RADIUS client transmitting request</td></tr><tr><td>Hostip</td><td>Local IP Address of RADIUS server</td></tr><tr><td>Accounttype</td><td>Service type name that was used to retrieve service type specific authorization attributes.</td></tr><tr><td>Amountleft</td><td>Remaining monetary account balance</td></tr><tr><td>dataleft</td><td>Data remaining in bytes</td></tr></table>

Dataleftlow	Data remaining in bytes (first 32-bits)
Datalefthigh	Data remaining in bytes (second 32-bits)
Destip	IP Address of system response is transmitted to
Code	Command code of RADIUS packet

Within each filter source the first time a variable is referenced all attributes associated with the source are assigned to variables. Subsequent additions of new attribute data is reflected in future variable references within the filter source. Deletion or changes to values of variable assignments however are not reflected in future references within the filter source. If a filter that removes an attribute is executed while the attribute is removed subsequent filters are still able to reference the attribute variable as it was prior to deletion.

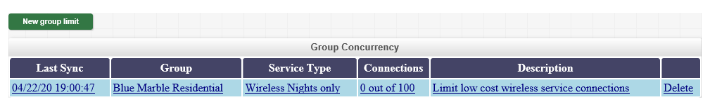
When merge operation is "Add attributes from query" a single result set containing following named columns is required. Columns VendorID, AttributeID, and Data must be present in result set. Tag column can be omitted if unused.

Column	Description
VendorID	Required Numeric Vendor ID of attribute. See Vendors.
AttributeID	Required Numeric Attribute ID of attribute. See Vendor Attributes.
Tag	Optional numeric tag value for grouping tagged attributes. If attribute is not tagged or tag out of range (1-31) tag value is ignored.
Data	Required Attribute value

If in one or more rows of result set VendorID and AttributeID are both 0 the request is rejected. The Data column may optional contain a failure message to be transmitted via Reply-Message attribute.

If in one or more rows of result set VendorID and AttributeID are both -1 an Access-Reject response is converted to Access-Accept. This is applicable only for RADIUS proxy.

Group Concurrency

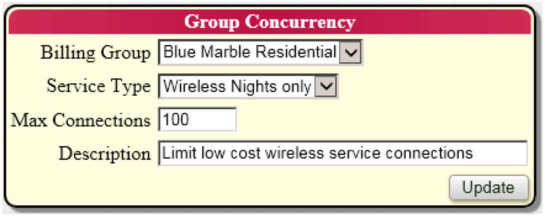


Concurrency control is widely used on a per account basis to restrict the number of concurrent sessions any single account is allowed to have. This serves to prevent abuse by discouraging sharing of the access account with others. Group concurrency takes the same idea of restricting concurrent access but applies it at the service type and billing group level. This may be useful for cases where a billing group belongs to a company that may not be allowed to use more than a set number of concurrent sessions at any one time across all of the group's accounts.

If group concurrency is in use both the users per account concurrent session limit and the group concurrency limit apply. In order for concurrency control to be enforced the "(Auth) Concurrency control" option within "Advanced" menu of RadiusNT/X administrator must be enabled.

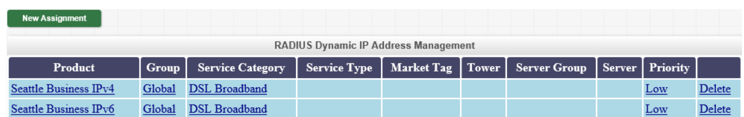
If multiple overlapping group concurrency restrictions apply to a single subset of accounts the most restrictive setting is honored.

Enforcement and accuracy of concurrency control depends on complete and timely receipt of accounting records from all access devices. If you are using an outsourced provider for network access please check with them to ensure they offer a robust RADIUS accounting retry policy.



Field	Description
Billing Group	Billing group concurrency restriction is to apply.
Service Type	Optional service type the concurrency restriction is to apply. When "All" concurrency restriction applies to all accounts within the billing group.
Max Connections	Maximum number of allowed concurrent sessions
Description	Text uniquely describing purpose of the group concurrency restriction.

Dynamic Addressing



Product	Group	Service Category	Service Type	Market Tag	Tower	Server Group	Server	Priority	
Seattle Business IPv4	Global	DSL Broadband						Low	Delete
Seattle Business IPv6	Global	DSL Broadband						Low	Delete

Dynamic addressing assigns IP addresses to RADIUS authenticated users from inventory on demand during the authentication process. At the end of the session inventory is automatically unassigned and made available for use by future sessions.

Where possible we recommend avoiding the use of this feature. As an alternative it is recommended longer term static assignment or use of NAS/controller based address pools or DHCP be utilized. These methods are closer to the network and likely to provide most reliable level of service.

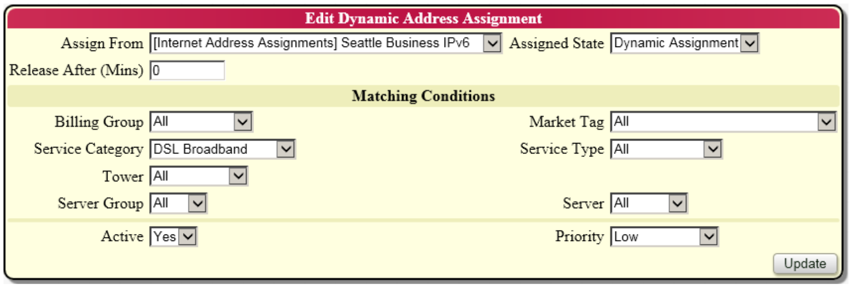
Emerald managed dynamic addressing is dependent entirely upon RADIUS signaling between Emerald and the NAS. For proper operation it is critical each NAS be configured with a robust retransmission policy for RADIUS accounting to ensure reliable receipt of accounting data. Where supported by NAS we recommend that interim accounting and session manager session verification (CoA probe) is used in conjunction with this feature.

In absence of reliable data addresses currently in use may be incorrectly deemed to be unused and returned to inventory possibly leading to duplicate assignment. Alternately addresses no longer used may remain allocated indefinitely unnecessarily reducing availability of addresses within inventory.

Before dynamic address management can be performed following pre-requisites are required:

- RadiusNT/X 6.0.13 or later
- NAS configured to transmit at least RADIUS Accounting start and stop indications
- "(Auth) IP Pooling" enabled from advanced menu of RadiusNT/X Administrator
- Emerald Scheduled task "Update RADIUS dynamic addressing" activated

When multiple competing dynamic addresses are defined the best match for each address family (e.g. IPv4, IPv6 .etc) is automatically selected based on assignment having the highest priority followed by assignment with most specific matching criteria. Multiple assignments can be allocated concurrently for the same session to support dual stack deployment however only one assignment per address family is allowed.



Field	Description
Assign From	[Product](#) from inventory addresses items are to be allocated from. Only products associated with [product sources](#) having source types of 'IPv4 Reservation','IPv6 Reservation' or 'Integer Reservation' are available for selection.
Assigned State	Upon assignment of an address from inventory this determines what assigned state of the inventory item shall become. Unlike static allocations the inventory state type used for dynamic allocation is 'Unavailable' rather than 'Assigned'. Recommended an inventory state labeled 'Dynamic Assignment' or similar be created using a state type of 'Unavailable' for use specifically in conjunction with dynamic allocation. This helps to document and more easily understand utilization of address resources within the inventory system.
Release After	Intended to manage assumptions of session state occurring between initial RADIUS authentication and receipt of subsequent RADIUS accounting start data. A higher value increases the time inventory is allowed to remain allocated without initial receipt of RADIUS accounting start message from NAS. Too high a value can cause inventory to remain allocated for longer than necessary reducing available address resources for assignment. Too low a value can cause inventory to be marked as available which is in use possibly leading to duplicate address assignment. It is recommended a setting of between 5 and 60 minutes is used. Following lists possible circumstances that could impact configuration decisions: • A successfully RADIUS authenticated session may not be granted access by the NAS itself and therefore IP can be allocated by Emerald yet never used by NAS and no subsequent session start indication ever transmitted. • Indication of successfully RADIUS authenticated session (Access-Accept) may not reach the NAS due to proxy, network or systems conditions. • RADIUS start requests may be delayed / queued internally within NAS for transmission thus delaying Emerald's knowledge of the session having started. • RADIUS start requests may be queued for upload within RadiusNT/X thus also delaying Emerald's knowledge of session start.
Billing Group	Limits assignment to services within selected billing group
Market Tag	Limits assignment to services having corresponding active MBR or Service level tag
Service Category	Limits assignment to services within chosen service category

Service Type	Limits assignment to services of chosen service type
Tower	Limits assignment to services assigned to selected tower
Server Group	Limit assignment to services authenticated from NAS belonged to selected server group
Server	Limit assignment to services authenticated from chosen NAS
Active	When 'Yes' new assignments can be made using this configuration. When 'No' new assignments are not performed however as existing assignments are closed inventory will continue to be restored to an available state even while active is 'No'.
Priority	When multiple assignments of the same address family are able to be selected for assignment this provides a means of explicitly indicating a preference of which assignment should be favored. Highest priority assignments are favored over lower priority assignments. If multiple assignments of the same address family have the same priority the system selects the most "specific" match based on the assignment imposing strictest constraints.

Clear Online List

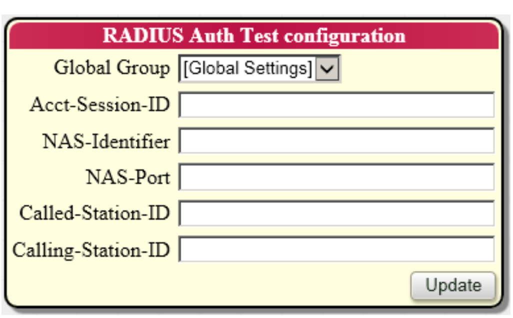
Active session list as show in "Emerald Client" / "Reports" / "Online" can be manually cleared globally or on a per NAS basis as needed from this menu. Clearing the list does not cause active sessions to be physically disconnected. Once the list is cleared active sessions will be restored to the online list upon receipt of the next Interim accounting update or if Interim accounting updates are unavailable at the start of users next session.

It is recommended the online list be cleared whenever RadiusNT/X has been offline for an extended period of time due to a network or systems outage or when there is reason to suspect a substantial number of RADIUS accounting stop records have been lost. Clearing the online list should not be done when rebooting a network access server as long as the access server transmits Accounting-On and or Accounting-Off notifications on reboot Emerald is automatically able to clear affected sessions in this case.

Field	Description
NAS Identifier	When "All" all sessions globally in the online list are cleared otherwise only sessions associated with selected NAS are cleared.

```
When using access servers supporting RADIUS dynamic authorization the feature
"Verify Session Status" in access server configuration can be used to
automatically clear sessions in the event of incomplete RADIUS accounting
data.
```

Auth Test Config



This menu option sets optional session identifying RADIUS request attributes used in conjunction with Auth Test feature within a services RADIUS menu. Auth test performs test

RADIUS authentications from within Emerald for troubleshooting purposes.

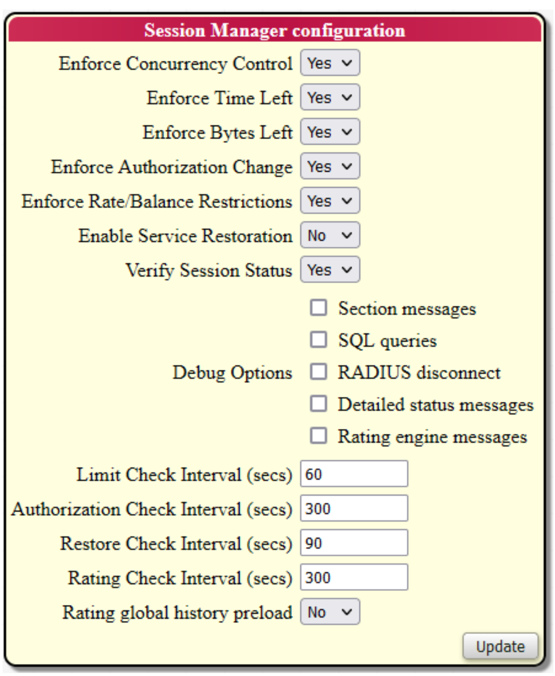
```
If special restrictions such as server access rules exist configuring session
identifying attributes can be configured to allow testing to succeed.
```

Session Manager

Session manager continually monitors active RADIUS sessions as shown in Emerald online report for violations of defined access limits or updated authorization parameters issuing either change of authorization or disconnect to limit leakage or update a sessions authorization.

In some environments session manager may not be necessary as sufficient limits are often able to be enforced by RADIUS reply attributes transmitted during initial session authorization such as Acct-Session-Time used to limit duration of a session. Other features such as concurrency control prevent same account from establishing multiple sessions at the same time.

To use the session manager on the windows platform "Emerald Session Manger" service must be started and configured to start automatically from Windows services manager. On UNIX platforms the /usr/local/emerald/sesmgr program should be started. Running "sesmgr –debug" from folder Emerald has been installed to will start the session manager in debug mode allowing you to view detailed information on any actions taken by session manager. Session manager can be run in simulated mode where rather than disconnecting sessions the actions it would normally take are displayed on screen by including flag '-disarm' when running sesmgr manually.



All access servers receiving disconnect requests must support RFC3576 disconnect messages and be configured to allow disconnect requests from IP address of Emerald server running session manager. Additionally each access server and its CoA/Disconnect port must be configured in Emerald via the Emerald Admin / RADIUS / Access Servers menu.

The following are examples of situations where session manager can offer value beyond initial authorization attributes transmitted at start of session:

- Enforcement of session time and data restrictions (Time Left and Data Left fields in the MBR services menu) when concurrency control is not enforced or where accounts are otherwise allowed to have multiple sessions active at the same time.

- Enforcement of data and rating/account balance based restrictions such as monthly total data usage limits. In order to disconnect active sessions after a set amount of data usage has been reached it is important the access server is configured to send RADIUS Accounting Interim update records to RadiusNT/X on a regular basis. See Emerald Admin / Rating / Rule Sets for more information on configuring data usage restrictions.

- Session manager provides an alternate method of concurrent access control. Typically concurrent access is controlled during authentication. RadiusNT/X checks list of online users and if user is already online they are not allowed to login a second time. This method may incorrectly deny access by determining a user is already online when they are not due to delay in receipt or loss of RADIUS accounting messages. The session manager allows authentication to proceed however after a short time later upon any concurrency violation the oldest active session is disconnected.

- Changes to user's account occurring after they have authenticated such as upgrade or downgrade of service, cancellation, NSF/dishonored payment or expiration of related add-on services are able to be enforced automatically using session manager without manual operator intervention.

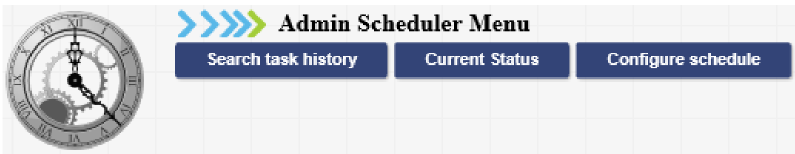
Field	Description
Enforce Concurrency Control	When enabled session manager enforces account login limit restrictions. If number of allowed concurrent sessions is exceeded then oldest existing session is disconnected. Only per account concurrency restrictions are enforced. Group based concurrency control is not.
Enforce Time Left	When enabled session manager enforces account time left restrictions
Enforce Bytes Left	When enabled session manager enforces account data left restrictions
Enforce Authorization Change	When enabled changes to user RADIUS attributes while users session is active such as upgrading or downgrading service, payment or expiration of child services, active market tags and assigned inventory will cause an automatic disconnect to enable session to be reestablished with updated authorization attributes.
Enforce Rate/Balance Restrictions	When enabled the session manager disconnects sessions by checking usage of all open sessions for the account against the configured rating rules. If there is no time remaining or an authentication reject rule applies (See Rating upload attributes in the Rating section of this document) the session is disconnected. If change of rating authorization parameters via upload attributes is detected a change of authorization (CoA) message will be sent with new authorization parameters. If the CoA request is not successful a session disconnect is then issued.
Enable Service Restoration	In cases where RADIUS authentication has failed due to service expiration yet limited access is allowed to facilitate notification or payment this feature disconnects limited access sessions once it is detected service has become active and no longer expired. After having been disconnected clients have the opportunity to re-authenticate in order to regain normal access. To use this feature service type level auth fail attributes should be configured with failure reason of service expiration. If failure attributes are not being used and expired sessions are to be denied access this feature should be disabled. Username for authentication should be unique within the system. NAS support for Class attribute is necessary to properly disambiguate limited access from normal access sessions. When enabled "Restore Check Interval" below manages how often to check for

	unauthorized sessions that become active after having previously been expired.
Verify Session Status	When enabled and 'Verify Session Status' is configured for Access Servers from RADIUS menu session manager periodically confirms active status of each session with each enabled access server. This feature is able to automatically detect situations where a session may no longer be active even though no RADIUS Accounting stop message was received and therefore session is assumed active from perspective of Emerald online report. Confirmation is achieved by periodically transmitting CoA requests to access servers for each active session. Access servers must support RFC5176 dynamic authorization to use this feature. If CoA request returns Error-Cause = Session-Context-Not-Found then session is removed from online list. Upon success or receipt of any other Error-Cause existing session is assumed to be currently valid and shall not be removed.
Debug Options	When running in the background as a windows service or detached process on UNIX systems debug options control level of detail about session manager activities written to session manager log file (sesmgr.log by default) located in the log sub directory of the emerald folder. Normally it is recommended that all debug options remain disabled unless needed. Any error or warning conditions that occur are unconditionally written to the sesmgr.log file.
Limit Check Interval	Number of seconds between checks of all active sessions for time left or concurrency violations. This must not be set lower than 20 seconds.
Authorization Check Interval	Number of seconds between checks of active sessions for changes to user authorization attributes.
Restore Check Interval	Number of seconds between checks of unauthorized sessions that become active after having previously been expired as managed by "Enable Service Restoration" feature above.
Rating Check Interval	Number of seconds between checks of all active sessions for rating rule violations as described by Enforce Rate/Balance Restrictions above. This must not be set lower than 20 seconds.
Rating global history preload	If Rating/Balance restrictions are enforced and rating rules require access to historical summary data to account for usage this controls whether the information is retrieved per account "No" or globally "Yes" as necessary. Enabling this option may improve performance of the Emerald system at the expense of possibly slightly outdated summary data. The default recommended value is "No".

```
Before enabling session manager confirm dynamic authorization between Emerald
and Access servers is working properly.  This can be achieved using Emerald
online report to disconnect test sessions on each server.  When able to
successfully disconnect sessions from online report within Emerald Client /
Reports menu the session manager shall also be successful.  Any configuration
difficulty preventing successful disconnection of sessions from online list
also hinder session manager from operating properly.
```

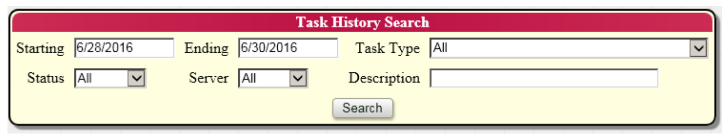
SCHEDULER

Emerald scheduler executes recurring and one-time on-demand tasks to automate management of billing and maintenance activities. Processes automated by scheduler include invoice and statement creation, email, statement delivery, notifications, automatic credit card billing, usage billing, external system synchronization, geography, log, system and account maintenance.



Search Task History

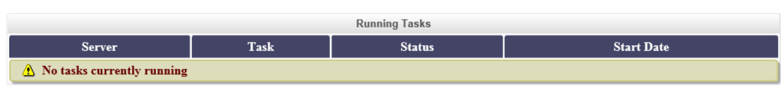
Task history search allows history of completed tasks and execution results to be reviewed.



Field	Description
Starting	Matching tasks completed on or after given date will be included in search results.
Ending	Matching tasks complete prior to given date will be included in search results.
Status	When not "All" results are filtered by execution status of task
Server	When not "All" results are filtered by Emerald scheduler server that processed the task.
Task Type	When not "All" results are filtered by selected task type
Description	When not empty results can be filtered by task description. Search is non-case sensitive and is performed as a substring search. For example entering "clear" will return all task entries with a description that contains the word "clear".

Current Status

Current status provides current information about the progress and state of currently running tasks. For example if a credit card batch export is currently running statistics are periodically updated showing current number of processed transactions and cumulative approval and decline totals.



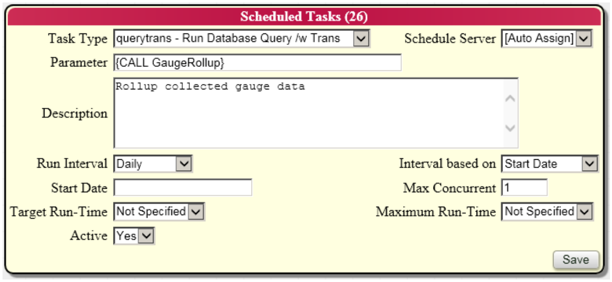
Configure Schedules

Scheduled tasks are managed from configure schedules menu. Any "One Time" tasks configured in this menu are automatically removed from view once the task has completed.


New Task

Scheduled Tasks

ID	Task Name	Description	Active	Aligned	Interval	Start	Server	Options
13	batchexport	Export CC/EFT transactions	No	No	1/4 Day		Auto Assign	Delete
243	ews	Process service monitoring	No	No	5 Minutes		Auto Assign	Delete
18	ews	Geographic match address coordinates by layer	Yes	No	1/4 Day	01/01/00 14:55	Auto Assign	Delete
74	geoexport	Geocode accounts with new or updated address information	Yes	No	1 Hour		Auto Assign	Delete
310	ipam	Process address group inventory allocation	Yes	No	10 Minutes		Auto Assign	Delete
76	query	Rollup collected gauge data	Yes	Yes	Daily		Auto Assign	Delete
60	query	Trim and deduplicate RADIUS logs	Yes	Yes	30 Minutes		Auto Assign	Delete
17	query	Determine called location for voice calls	No	No	Daily		Auto Assign	Delete
12	query	Incidents incremental FTS reindex	Yes	Yes	1/4 Day	09/22/09 00:00:48	Auto Assign	Delete
4	query	Trim database logs	Yes	Yes	Daily	09/22/09 02:40:48	Auto Assign	Delete
3	query	Trim calls	Yes	Yes	1/4 Day	09/22/09 02:20:48	Auto Assign	Delete
2	query	Check database	Yes	Yes	Weekly	09/22/09 03:17:48	Auto Assign	Delete
311	querytrans	Update RADIUS dynamic addressing	No	No	5 Minutes		Auto Assign	Delete
265	querytrans	Process late fees	Yes	Yes	Daily		Auto Assign	Delete
211	querytrans	Gapless invoice numbering data collector	Yes	Yes	Daily		Auto Assign	Delete
75	querytrans	Process customer referrals	Yes	Yes	Daily		Auto Assign	Delete
65	querytrans	Update accounts with scheduled changes	Yes	Yes	Daily		Auto Assign	Delete
15	querytrans	Update Reseller Usage	Yes	No	1/4 Day		Auto Assign	Delete
14	querytrans	Void auth only transactions not captured within 10 days	Yes	No	Daily		Auto Assign	Delete
9	querytrans	Inactivate Canceled Accounts	Yes	Yes	Daily	09/22/09 00:45:48	Auto Assign	Delete
1	querytrans	Update account timebank	Yes	Yes	Daily		Auto Assign	Delete
16	taskautoclose	Expired MBR Auto Close	No	No	Daily		Auto Assign	Delete
8	taskemailinvoice	Email Invoices	No	Yes	Daily	09/22/09 00:00:48	Auto Assign	Delete
11	taskemailstatement	Email Statements	No	Yes	Daily	09/22/09 00:00:48	Auto Assign	Delete
6	taskinvoice	Create Invoices	No	Yes	Daily	09/22/09 06:00:48	Auto Assign	Delete
66	taskmarketactive	Updates account market tag status	Yes	Yes	Daily		Auto Assign	Delete
5	taskratecharges	Create Usage Charges	No	Yes	Daily	09/22/09 05:00:48	Auto Assign	Delete
7	taskstatement	Create Statements	No	Yes	Daily	09/22/09 07:00:48	Auto Assign	Delete



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Task Type</td><td>The following task types are available:
<table>
<tr><th>Task Type</th><th>Description</th><th>Parameters</th></tr>
<tr><td>batchexport</td><td>Export CC/EFT Transactions</td><td>Optional (raw)
CustomerID or CustomerID:BatchProcessorID

Optional(key=value,)
CustomerID=x,
BatchProcessorID=y,
partid=a,
parts=z

partid and parts are used to partition large batches of CC/EFT transactions into multiple smaller tasks. Parts refer to the total number of partitions and partid refers to the partition number assigned to the scheduled task.

To split batch workload between two scheduled tasks A and B configure tasks with following parameters:

batchexport A: partid=1,parts=2
batchexport B: partid=2,parts=2

To further split work across three tasks A, B and C:

batchexport A: partid=1,parts=3
batchexport B: partid=2,parts=3
batchexport C: partid=3,parts=3

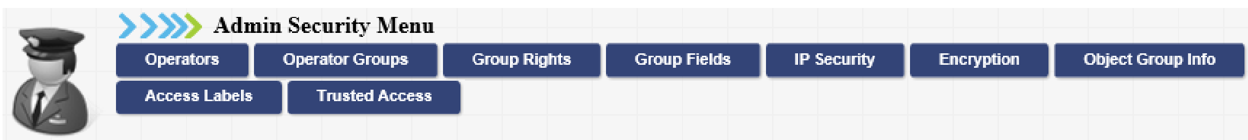
To ensure full batch processing of all customer transactions care should be taken to configure a parts number of batchexport tasks each corresponding with a unique partid.</td></tr>
<tr><td>batchimport</td><td>Import CC/EFT Transactions</td><td>Optional (raw)
CustomerID or CustomerID:BatchProcessorID</td></tr>
<tr><td>geoexport</td><td>Geocoder processing</td><td>Optional (key=value,)
CustomerID=x,
GeocoderID=y</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>userexport</td><td>Account export</td><td>Required (raw) ExternalSystemID</td></tr><tr><td>taskinvoice</td><td>Create Invoices</td><td>Optional (raw) GroupID</td></tr><tr><td>taskautoclose</td><td>Expired MBR Auto Close</td><td>No parameters</td></tr><tr><td>taskmarketactive</td><td>Update Market Tag Status</td><td>Optional (raw) GroupID</td></tr><tr><td>taskemailinvoice</td><td>Email Invoices</td><td>Optional (raw) GroupID</td></tr><tr><td>taskemailstatement</td><td>Email Statements</td><td>Optional (raw) GroupID</td></tr><tr><td>tasknotices</td><td>Run Notices</td><td>Required (raw) i+InternalID (e.g. i2) or NoticeID</td></tr><tr><td>ews</td><td>Run EWS template</td><td>Required (key=value,) File=ewsfile, ***Key=value - posted to Variables table</td></tr><tr><td>Query</td><td>Run Database Query</td><td>Required (raw) SQL Query</td></tr><tr><td>Querytrans</td><td>Run Database Query /w Trans</td><td>Required (raw) SQL Query</td></tr><tr><td>taskstatement</td><td>Create Statements</td><td>Optional (raw) GroupID</td></tr><tr><td>taskratecharges</td><td>Create Usage Charges</td><td>No parameters</td></tr><tr><td>taskratedata</td><td>Rate Data Source</td><td>Required (raw) RateDataSourceID</td></tr></table>
Schedule Server	In cases where Emerald server software runs across multiple systems tasks can be assigned to execute on those specific systems or set "Auto Assign" to allow Scheduler to make the appropriate assignment decision.
Parameter	Please see the parameter field of "task type" above for details on parameters accepted for a given task type.
Description	Optionally enter a description of the scheduled task.
Run Interval	Choose the appropriate interval recurring tasks should be run.
Interval based on	When "Start Date" the task always runs on the same recurring interval based on the starting date. When "Last Run Date" the interval is based on time of last completion of task. For example if run interval is 60 minutes and it takes 20 minutes for a task to run - With "Start Date" the task runs 40 minutes after last completion to maintain alignment with initial start date. With "Last Run Date" the task runs 60 minutes after last completion.
Start Date	Enter the initial Start date and time of the task.
Max Concurrent	Enter the maximum number of instances of this task that can be running at any one time.
Retries	If the task fails it is immediately retried with no backoff period between attempts up to selected number of times until task completes successfully or retry limit is reached. This feature is intended to reduce processing latency when transient conditions preventing a task from completing are encountered and should be used sparingly. Normally when retries are not set any work not processed previously would be picked up in the future next time the task runs.
Maximum Run-	Limits runtime of tasks in a single session. For task types query and querytrans maximum

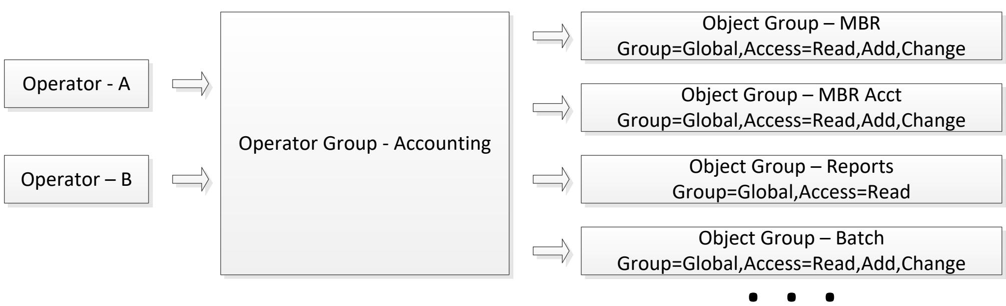
Time	runtime is applied as query timeout. For notices, geocoder and CC/EFT export batches processing is suspended once runtime limit is reached. This field is ignored for ews, invoice, statement and qsync tasks.
Active	While a task is inactivated it will no longer be scheduled to be run again in the future. If the task is already running task execution will soon be canceled when possible. After inactivating a task you don't want to run click "Apply" so that schedulers are refreshed with new configuration. For development, testing or decommissioning upgrade & testing safing is recommended instead of relying on scheduled tasks not to run.

SECURITY

Operators, related access controls and system level security features are managed from the security menu.

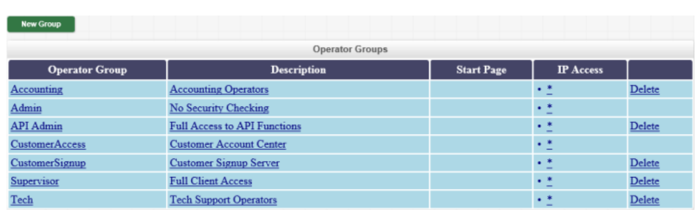


Access security in Emerald is group based similar to operating system user account management. Operators are assigned to operator groups where access rights are determined by "object groups" assigned to each operator group.



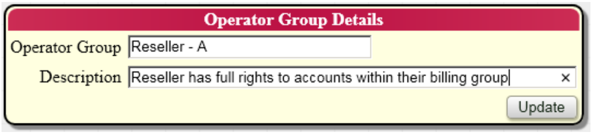
Operator Groups

Operator Groups define a collection of access privileges controlling what operators are able to access once logged on to Emerald. IP access security is also configurable by operator group restricting access to approved networks. The "Admin" operator group is a special group where all object access checking is disabled. Operators assigned to the admin group have unrestricted access to Emerald. Some features within Emerald Administrator require operators to be members of the admin group to configure.


New Group

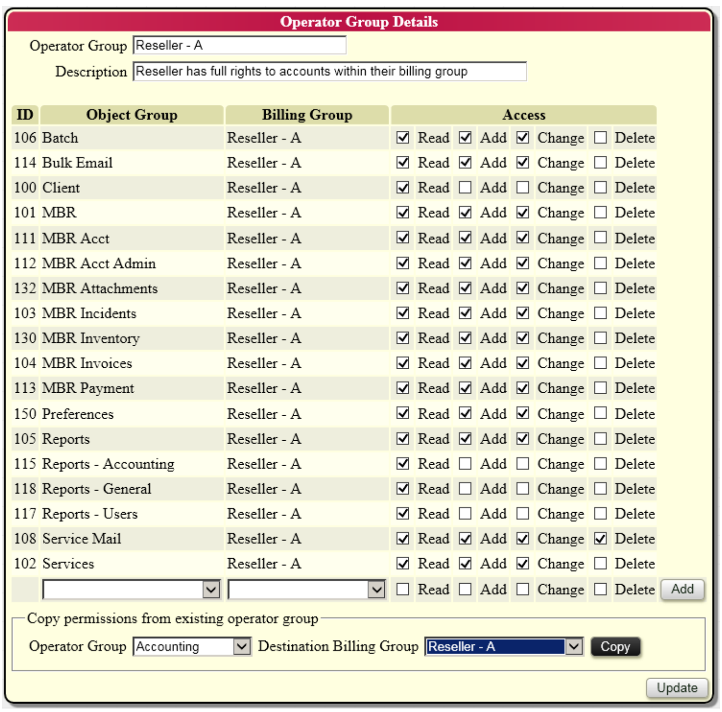
Operator Groups

Operator Group	Description	Start Page	IP Access	
Accounting	Accounting Operators		• *	Delete
Admin	No Security Checking		• *	
API Admin	Full Access to API Functions		• *	Delete
CustomerAccess	Customer Account Center		• *	
CustomerSignup	Customer Signup Server		• *	Delete
Supervisor	Full Client Access		• *	Delete
Tech	Tech Support Operators		• *	Delete



Field	Description
Operator Group	Unique identifying descriptive name for the operator group. This will be presented when assigning operators to operator groups within the Operators menu.
Description	Enter a longer description or comment regarding the operator group entry.

Once an operator group has been created additional fields are presented to manage assignment of access rights to the group.



Field	Description
Object Group	Identifies areas within the system the operator group is to be granted access. For a complete list of all available object groups with a description of access they provide select "Object Group Info" link from "Emerald Admin" / "Security". If you will be doing a lot of security management you may want to print this information out to keep as a reference guide. Object groups are managed from the "Emerald Admin" / "Advanced" / "Object Groups" menu. Configuration of object groups is not supported.
Billing Group	When billing group is "Global" access permission applies across all billing groups throughout Emerald. Otherwise access permission applies only to MBRs and services within the matching billing group. Reseller operators will typically be assigned access only to specific billing groups allowing them to manage only their subset of accounts.

<table>
<tr><td></td><td>Several Administrative object groups provide access to system configuration unrelated to management of accounts. For these items assigning a specific billing group provides no limits on display or configuration of data in these areas.</td></tr>
<tr><td>Access</td><td>Select the appropriate access privilege to be applied to for the object group. To remove entries from the list uncheck all access privileges.

<table>
<tr><th>Access</th><th>Description</th></tr>
<tr><td>Read</td><td>Permits data to be displayed but not read. Read is sometimes a prerequisite required before data can be modified or removed.</td></tr>
<tr><td>Add</td><td>Permits new records to be added</td></tr>
<tr><td>Change</td><td>Permits existing data to be modified</td></tr>
<tr><td>Delete</td><td>Permits permanent removal of data</td></tr>
</table></td></tr>
<tr><td>Copy permissions</td><td>Enables access rights associated with an existing operator group to be copied into this group. This is often used while creating new operator groups with similar functionality to an existing group. Once configuration is copied custom changes which differentiate groups can then be applied.

Copy permissions are also useful in reseller environments where operators are restricted to managing accounts within their billing group only. By selecting a billing group when copying configuration the billing group level restrictions can be automatically applied.</td></tr>
</table>

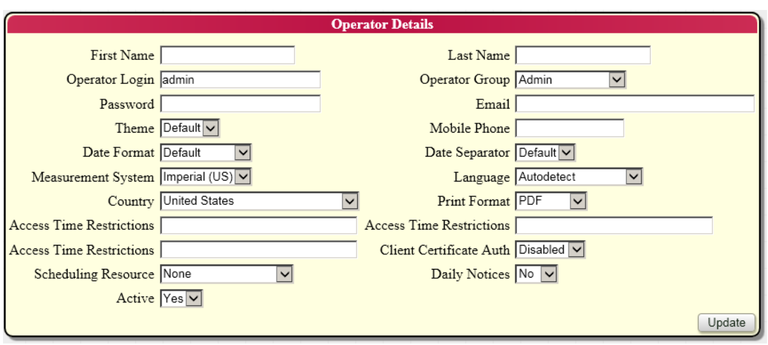
Operators

Access accounts required for operators to login to Emerald are configured from operators. Prior to creating new operator accounts it is recommended operator groups be reviewed to make sure expected access rights will be granted to your new operators. By default admin operator account is created with a password of "pass1". This should be changed as soon as possible when logging on to Emerald for the first time.


New Operator

Operators

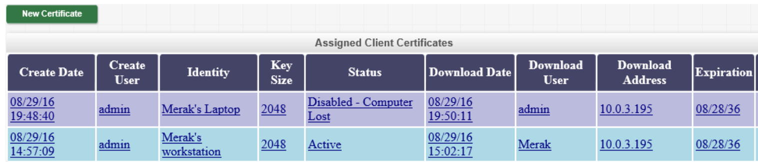
Operator	Name	Group	Contact	Access Time	Cert Auth	Theme	Language	Measures	Printing	
admin		Admin			Required	desk	Auto	Imperial (US)	HTML	
Maia		Accounting		• Mon-Fri 8:00 AM - 6:00 PM	Disabled		Auto	Imperial (US)	HTML	Delete
Merak		Tech		• Mon-Fri 8:00 AM - 6:00 PM	Disabled		Auto	Imperial (US)	HTML	Delete
Merope		Supervisor			Disabled		Auto	Imperial (US)	HTML	Delete
signup		CustomerSignup			Disabled	bluemarble	Auto	Imperial (US)	PDF	Delete



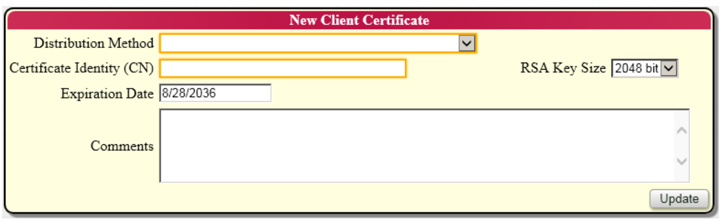
Field	Description
First Name	Operator name (informational only)
Last Name	Operator name (informational only)
Operator Login	Unique login name identifying the operator. This value will be presented as identification when selecting operators throughout Emerald as well as any audit or change logging.
Operator Group	Operator group determines access rights granted to this operator.
Password	Operators access password. Content of the operator password field is not masked when initially entered yet subsequently never visible when the operator is displayed in the future

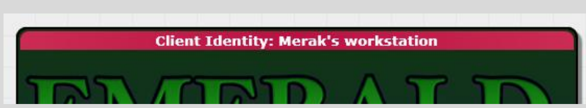
	regardless of the systems password visibility rules. If Emerald database field encryption is not enabled operators passwords are stored in the clear within Operators table of Emerald database.
Password Change	When 'Requested' operators are prompted upon logging on to change their passwords or to contact their administrator if they do not have access to password change. This is a request; operators may continue to use Emerald without changing their passwords. In the operator listing operators appearing with red background color have been requested to change their passwords but have not yet done so. This setting changes the value of PasswordChange to 1 in the Operators table.
Email	Email address is used for operator based notifications
Mobile Phone	Mobile phone number used for operator based SMS notification
Theme	Operators preferred theme. When a non-default theme is selected value of 10000000 is added to theme score expressing operators preferred theme. If other themes include criteria scoring higher then operators preferred theme is not used.
Date Format	Operators preferred date format for rendering of date fields. Date format can be changed by the operator after logging on from "Emerald Client" / "Options".
Date Separator	Operators preferred date part separator for rendering date fields. Separator can be changed by the operator after logging on from "Emerald Client" / "Options".
Measurement System	Determines whether units of distance and weight should be presented using Imperial or Metric systems. Measurement system can be changed by the operator after logging on from "Emerald Client" / "Options"
Language	Sets language of Emerald client operator interface. When "Auto detect" browsers stated language preferences are used to determine best matching language to display. Localization is only available for Emerald client interface, signup and customer center interfaces.
Country	Country operator and most of the operator's accounts are located. The current use of country is to define the local calling area for Caller-ID based account searches.
Print Format	Default print format for displaying contents of reports. Selected print format may be substituted automatically based on capabilities of enabled reporting systems. Print format can be changed by the operator after logging on from "Emerald Client" / "Options"
Access Time Restrictions	When not blank operator will only be able to access Emerald within configured access time. Please see Common fields for formatting details.
Client Certificate Auth	When "Required" client certificate authentication is required when logging on as this operator. Please review Assigned Client Certificates below for more information before enabling client certificate authentication. If necessary certificate authentication may be disabled for operators outside of Emerald by executing Emerald database stored procedure "CertToggle 'operator',0" where "operator" is the operator login from a database query tool. When "Disabled" certificate authentication is not required and outcome of any certificate authentication is ignored.
Scheduling Resource	If operator will be assigned appointments this determines scheduling resource operator is able to receive assignments from. Once a scheduling resource has been selected operator availability is be configured below. Assignment also requires operator to be assigned to the appropriate operator roles.
Daily Notices	Indicates whether operator should receive notices sent on a daily basis if any have been configured.
Active	"Yes" - operator is able to access Emerald. "No" - operator cannot login. An operator currently logged on at the time their account is inactivated is automatically logged off within 5 minutes. If necessary active operators can be disconnected immediately from "Emerald Admin" / "Web Interface" / "Active Sessions".

Assigned Client Certificates



Once an operator account is created with "Client Certificate Auth" set "Required" the assigned certificates menu is available to manage distribution of client certs for multifactor authentication. Before certificates can be created a certificate authority (CA) must first be generated from Client Auth CA menu of Emerald configuration server. It is recommended a client certificate be generated for each device the operator will be using to access Emerald.



Field	Description
Distribution Method	Client certificates generated by Emerald are distributed in PKCS 12 format supported by most web browsers. Operators creating this certificate can chose to download and provide/install on behalf of the user or users can be given the opportunity to download certificate themselves upon next login. Regardless of distribution method certificate file may only be downloaded once. If a certificate is lost it can never be downloaded again in the future. Instead the certificate is disabled and a replacement issued in its place. Generated client certificate file contains public and private key pairs and should be handled with care.
Certificate Identity (CN)	Configures unique common name (CN) of generated certificate. It is recommended common name describe both individual it is assigned and if applicable identify specific system it is intended to be used with. Once saved CN is set forever and cannot be changed, deleted, reused or reissued. If there is a need to reissue a certificate a different common name must be chosen.  Upon successful client authentication common name appear as "Client Identity" in the banner at the top of the Emerald login dialogue.
RSA Key Size	Selects generated certificates RSA private key size in bits. May be either 2048 or 4096. Default recommended setting is 2048 bits.
Expiration Date	Sets an expiration period after which client certificate will no longer be valid. Once expired operator will not be able to access Emerald using this certificate.
Status	After initial certificate creation status allows access to Emerald using this certificate to be enabled or disabled. When disabled listed reasons can be managed from "Emerald Admin" / "Advanced" / "Client Cert Status".
Comments	Related additional information about certificate deployment or status

```
Once client certificate has been installed it is often necessary to close and
restart the browser before certificate is used.
```

PIV SMART CARD PROVISIONING – PIVKEY

As an alternative to loading client certificates into the browser or operating systems certificate store certificates may also be loaded into physical smart cards or USB keys for added security. To optionally provision a PIV card with an operator's client certificate generated above use the following steps. While these instructions are specific to PivKey steps are similar for PIV cards offered by other vendors.

1. Plugin reader and insert card

2. Install the vendor's miniport and tools (pivkey admin) this enables access to manage features of the card. This software is used only to initially configure the card and does not need to be installed by operators for subsequent use.

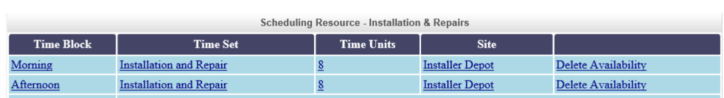
3. From windows registry editor under "HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Cryptography \ Defaults \ Provider \ Microsoft Base Smart Card Crypto Provider" add the keys "AllowPrivateExchangeKeyImport" and "AllowPrivateSignatureKeyImport" each with a 32-bit DWORD value of 1.

4. Load client certificate client.p12 downloaded from Emerald onto the card using the following command: **certutil -v -csp "Microsoft Base Smart Card Crypto Provider" -p "" -importpfx client.p12**

5. Finally configure card to mark loaded certificate as the default for client authentication: **"c:\Program Files (x86)\PIVKey Installer\PIVKey Admin Tools\pivkeytool.exe" --mapdefault --userpin "000000"**

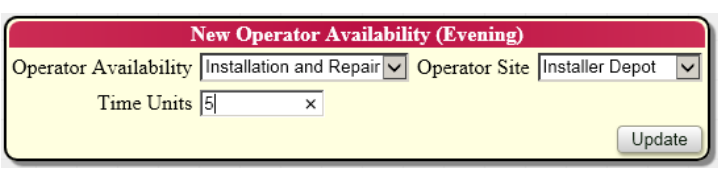
Physical smart cards are widely supported across operating systems, browsers and card readers without additional software. When card is plugged into reader operators are prompted to enter card pin when browsing to Emerald. Default PIN code for PivKey is **000000.**

Scheduling Resource


Scheduling Resource - Installation & Repairs

Time Block	Time Set	Time Units	Site	
Morning	Installation and Repair	8	Installer Depot	Delete Availability
Afternoon	Installation and Repair	8	Installer Depot	Delete Availability
Evening	Time block unassigned, click to assign block to operator			

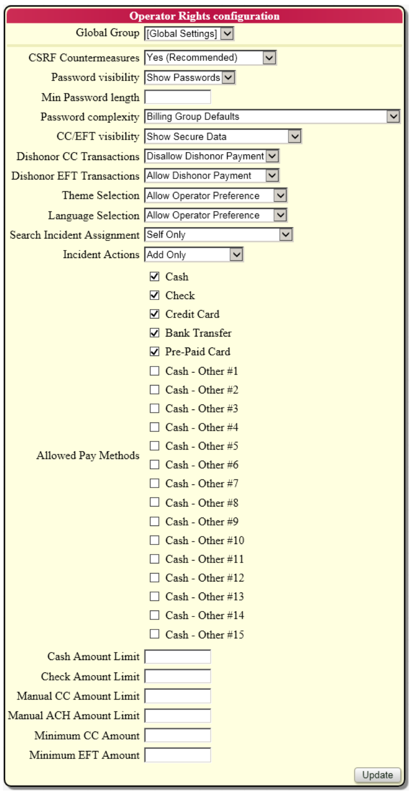
Once a scheduling resource has been chosen operator availability for receiving appointment assignments is configurable for each time block of the resource. If a scheduling resource is configured for an existing operator it is necessary to save the operator form before scheduling resource configuration is displayed.



Field	Description
Operator Availability	Scheduling time set corresponding with operators availability within given time block. For example if an operator is available for morning appointments every weekday then time set corresponding with "every weekday" is selected for the morning block.
Operator Site	Represents operators starting location for onsite appointment scheduling using roles with distance based assignment strategies or maximum distance limit.
Time Units	Units of time operator is available within the time block. Meaning of a "time unit" is operator defined relative to time units consumed by incident type. For more information see scheduling resources.

Group Rights

Various accounting limit and sensitive data visibility rules are configurable from the group rights menu on a global and per "Operator Group" basis.



Field	Description
Global Group	Controls the operator group the settings apply to. Settings of specific Operator Groups override "Global Settings". Operator groups having configurations separate from the global group display the "*" character by their name.
CSRF Countermeasures	Enables or disables cross-site request forgery (CSRF) protections. When countermeasures are enabled efforts are made to prevent this class of attacks however in doing so it may also prevent linking to specific areas of Emerald from external sites or emails that are not harmful. The following URL links are provided

	for safely linking to specific areas of Emerald from remote sites. **Link** / **Description** mbr.ews?CustomerID=x — Given an Emerald CustomerID this link displays a specific Emerald MBR. sa.ews?AccountID=x — Given a MBRs AccountID this link displays a specific Emerald MBR Service. incident.ews?IncidentID=x — Given an Emerald IncidentID this link displays the details of a specific Incident. invoice.ews?InvoiceID=x — Given an Emerald InvoiceID this link displays the details of a specific Invoice. stmt.ews?StatementID=x — Given an Emerald StatementID this link displays the details of a specific Statement. payment.ews?PaymentID=x — Given an Emerald PaymentID this link displays the details of a specific Payment.
Password visibility	Determines visibility for client MBR and Service passwords. When "Show Passwords" is set - clear text passwords are visible. When "Hide Passwords" is set a series of "*" characters is displayed in lieu of the password.
Min Password length	Minimum allowed MBR service password length. If configured any group level settings managed via client settings are overridden for applicable operator group(s).
Password complexity	Mixed case, letter, number and symbol requirements for service level passwords. If configured any group level settings managed via client settings are overridden for applicable operator group(s)
CC/EFT visibility	Determines visibility for client MBR and Service secure data fields such as Credit Card Number, SSN and bank account numbers. **Visibility** / **Description** Show secure data — Secure data fields are fully displayed without masking. Hide secure data — Secure data fields are completely masked. Show only last 4 — All but last four characters of a secure data field are masked. If secure data field is not large enough (4 or less characters) to accommodate this then masking automatically falls back to hide secure data. Show first 6 + last 4 — All but first 6 and last 4 characters of a secure data field are masked. If secure data field is not large enough 10 or less characters) to accommodate this then masking automatically falls back to show only last 4.
Dishonor CC Transactions	Determines whether operator is authorized to dishonor automatic CC payment transactions from within MBR payments menu. Operator must also have delete access to "MBR Payment" object group in order to dishonor payments.
Dishonor EFT Transactions	Determines whether operator is authorized to dishonor automatic EFT payment transactions from within MBR payments menu. Operator must also have delete access to "MBR Payment" object group in order to dishonor payments.
Parent Service Closing	When "Allow child services to remain open" the operator has the option of closing a parent service while leaving one or more child services open. When "Disallow child services from remaining open" all open child services are closed with the parent account without an option to exclude child services from closure. This setting is intended to reduce operator error and does not itself restrict an operator's ability to intentionally force a child service to reopen by other means such as directly manipulating its timeline or billing dates.
Theme Selection	Controls whether operator's client options menu displays a listing of available themes for the operator to choose from. If disabled only global administrators are

<table>
<tr><td></td><td>able to configure the operators chosen theme.</td></tr>
<tr><td>Language Selection</td><td>Controls whether operator’s client options menu displays a listing of available languages for the operator to choose from. If disabled only global administrators are able to configure the operators chosen language.</td></tr>
<tr><td>Organization Level Reporting</td><td>While running reports this setting manages criteria allowing operators lacking global MBR access to all billing groups to run organization level reporting.

Emerald enforces reporting access controls based on access to the report itself and upon Organization and Billing Group input parameters provided to reports. Reports themselves do not enforce access controls. A report run with the same set of input parameters always returns the same data regardless of who runs it.

This setting manages whether or not specified organizations via organization parameters are allowed without an accompanying billing group parameter.

Operators with insufficient group access to run reports at organization level generally have the option of running them for a specific billing group within the organization they have access.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Requires access to one or more groups of the organization</td><td>To run reports at organization level operators must be granted read access to at least one of the organizations billing groups.

Reporting can include data from billing group members of the organization the operator does not directly have read access.</td></tr>
<tr><td>Requires access to ALL groups of the organization</td><td>To run reports at organization level operators must be granted read access to each of the organizations billing groups.

An operator without read access to one or more of the organizations billing groups shall not be able to run organization level reports. This includes any unused billing groups that are no longer active.</td></tr>
<tr><td>Requires access to ALL active groups of the organization</td><td>To run reports at organization level operators must be granted read access to each of the organizations active billing groups.

An operator without read access to one or more of the organizations active billing groups shall not be able to run organization level reports.

If the organization contains no active billing groups then operators without global MBR access will not be able to run organization level reporting.

Reporting can include data from inactive billing groups within organization the operator does not directly have read access.</td></tr>
</table>
</td></tr>
<tr><td>Search Incident Assignment</td><td>When searching incidents from client support menu this controls search of incidents assigned to specific operators.

<table>
<tr><th>Search</th><th>Description</th></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td>Self Only</td><td>Operator can search incidents assigned to or created by them.</td></tr>
<tr><td>Operators /w Common Roles</td><td>Operators can search incidents assigned to other operators sharing a common operator role.</td></tr>
<tr><td>All operators</td><td>Operators can search incidents assigned to any operator.</td></tr>
</table>

These settings affect only list of operators present in assignment list when searching incidents. Access to incidents is governed exclusively by access controls associated with operators assigned operator group.</td></tr>
<tr><td>Incident Actions</td><td>Manages operator ability to modify incident actions. This setting is in addition to normal operator group level access configuration. To edit an action modify access must also be granted to "MBR Incidents" object group.

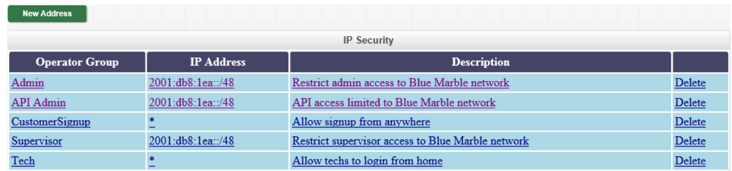
<table>
<tr><th>Access</th><th>Description</th></tr>
<tr><td>Add Only</td><td>Operators may add new actions to an incident. They may not make changes to any pre-existing actions.</td></tr>
<tr><td>Add & Change Self</td><td>Operators may add new actions to an incident and make changes to existing actions that the operator created.</td></tr>
<tr><td>Add & Change Any</td><td>Operators may add new actions to an incident and make changes to existing actions regardless of which operator created the action.</td></tr>
</table></td></tr>
<tr><td>Require PIN for MBR Access</td><td>When enabled operators are required to enter account PIN as it appears in the "Account PIN" field when editing an MBR. Prior to successful PIN entry operators are not able to access details of the MBR or make any changes to it. If no PIN is assigned the operator is granted access normally without being challenged for PIN entry.

When enabled expiration period is exclusively elapsed time since successful PIN entry. Once authorization expires the operator is again prompted to re-enter PIN to continue to access the MBR. Actual authorization time may vary by up to 15 additional minutes post selected expiration period.

This feature applies to the operator UI only and does not influence global operations such as batch invoicing, credit card processing, reports, post payments, bulk messaging or the Emerald API.

PIN entry is intended primarily as a means of enforcing customer account security by enforcing requirement to obtain a PIN code to authenticate customer prior to accessing or making changes to an MBR.</td></tr>
<tr><td>Allowed Pay Methods</td><td>Reflects pay methods operators are allowed to make against MBRs they manage.</td></tr>
<tr><td>Cash Amount Limit</td><td>Reflects maximum single cash payment amount operators are allowed to make against MBRs they manage.</td></tr>
<tr><td>Check Amount Limit</td><td>Reflects maximum single check payment amount operators are allowed to make against MBRs they manage.</td></tr>
<tr><td>Manual CC Amount Limit</td><td>When creating a manual credit card payment this sets maximum single payment amount operator is allowed.</td></tr>
<tr><td>Manual ACH Amount Limit</td><td>When creating a manual EFT payment this sets maximum single payment amount operator is allowed.</td></tr>
<tr><td>Minimum CC Amount</td><td>When creating a manual credit card payment this sets minimum single payment amount operator is allowed.</td></tr>
<tr><td>Minimum EFT Amount</td><td>When creating a manual EFT payment this sets minimum single payment amount operator is allowed.</td></tr>
</table>

IP Security



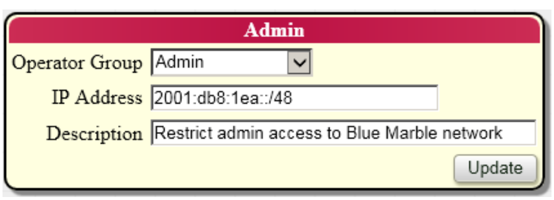
Operator Group	IP Address	Description	
Admin	2001:db8:1ea::/48	Restrict admin access to Blue Marble network	Delete
API Admin	2001:db8:1ea::/48	API access limited to Blue Marble network	Delete
CustomerSignup	*	Allow signup from anywhere	Delete
Supervisor	2001:db8:1ea::/48	Restrict supervisor access to Blue Marble network	Delete
Tech	*	Allow techs to login from home	Delete

IP security enables Emerald access to be conditionally restricted by IP address and operator group.

Access checking is performed in two steps. Initially client IP address is evaluated against all IP access rules across all operator groups. If there is no match IP access is unconditionally denied preventing access to non-static content including display of an initial login form. In the event access would be allowed by at least one operator group access to Emerald login form is allowed. Upon successful authentication operator group specific IP access rules are enforced.

Enforcement of IP Security requires "Enable IP access security" option to be enabled in the security menu of the Emerald configuration server. Regardless of IP security settings requests from the loopback source addresses "127.0.0.1" and "::1" are unconditionally allowed. If there should be a configuration error or change preventing network access operators may login to Emerald locally from Emerald server using localhost URL to make needed configuration changes.

When using Emerald in conjunction with non-transparent front end proxies please see reverse proxies to enable IP address pass thru.



Field	Description
Operator Group	When "All Groups" IP access rule is applied to all operator groups within Emerald. Otherwise the rule is applied only to the specified group.
IP Address	IP Address can reference a DNS hostname (user.mycompany.com) or valid IPv4 / IPv6 address range. Additionally the wildcard '*' is recognized to allow full IPv4 and IPv6 access.
Description	Enter description of the IP Address entry such as person or network being authorized.

Encryption

Encryption enables passwords and other sensitive information such as customer credit card and account numbers to be stored within Emerald database in a reversibly encrypted form. Encrypted storage provides following advantage:

- Protects sensitive information should database servers, backups or replicas become lost, stolen or copied.

Database encryption includes following risks:

- When password encryption is enabled external systems which access the Emerald database directly for password information will fail because they are not able to decrypt account password information. Any third party reporting system using an external renderer such as crystal reports will not be able to display contents of encrypted fields. Encryption is otherwise fully supported within Emerald with no loss of functionality when enabled.

- If encryption key is lost all encrypted data fields are also lost

Database encryption may not protect encrypted data fields under following general categories of circumstances:

- Compromise of currently active Emerald database to the extent data fields are able to be modified
- Compromise of Emerald software execution environment / operating system
- Compromise of integrity of data link between Emerald and database server
- Compromise of any middle boxes, proxies, firewalls that terminate TLS rather than passing through
- Compromise of any client system/operator using Emerald with sufficient access rights

Emerald encryption is based on the AES Rijndael algorithm using operator defined passphrase as secret key. Data fields are encrypted in a CBC mode with data authentication. Any two fields with same value encrypted with same secret key have the same encrypted output allowing anything with access to encrypted database to determine which if any accounts share same encrypted account numbers and passwords. This property enables certain synchronization and search operations on encrypted data to be performed by systems which do not possess encryption keys.

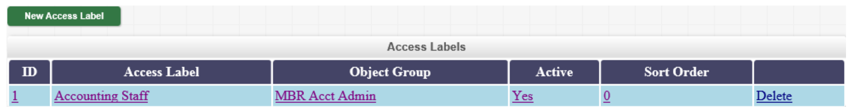
Once Emerald database is encrypted it can be decrypted later with the encryption passphrase. This allows changing encryption key or decrypting database for exporting data.

It is important to stress keeping a backup copy of encryption passphrase is extremely important. IEA Software has no way to recover any data encrypted with a lost passphrase. If the key is lost all data it protects is also lost.

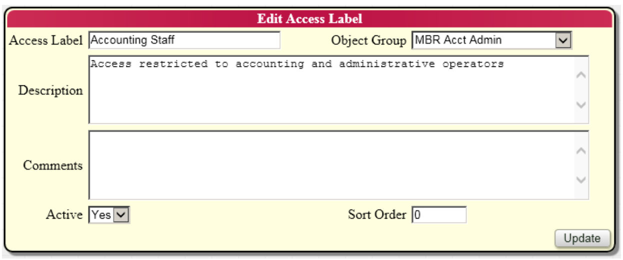
To encrypt or decrypt your database click "Emerald Admin" / "Security" / "Encryption" link and follow all instructions and warnings displayed. This process was designed to be done while the system is online with minimum amount of downtime.

Access Labels

Access labels are used primarily to apply access restrictions to account configuration options throughout Emerald.



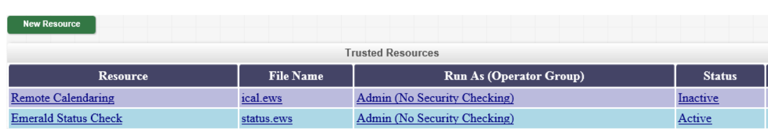
Access labels act as aliases of object groups. For example there is a need for accounts of service type "Wireless VIP" to only be created by "Supervisors". In this case an access label for supervisor level access is created by selecting an object group only supervisors are granted access to. Once the access label is generated it is assigned to Wireless VIP service from the [service types](#) menu. When completed operators who are not supervisors or global administrators will not see "Wireless VIP" service type for selection and are prevented from provisioning it.



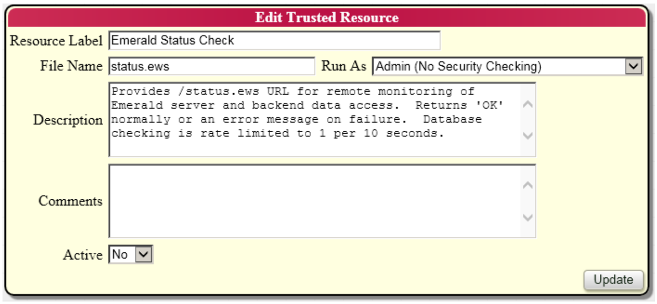
Field	Description
Access Label	Unique name for access label describing the type or level of access. This may be the same as selected object group.
Object Group	Object group an operator must be granted access to before any configuration items assigned to this access label may be selected.
Description	Additional details relating to use and purpose of this access label
Comments	Additional details relating to use and purpose of this access label
Active	When inactivated any configuration item associated with this access label will be inaccessible to all operators except those assigned to the admin operator group.
Sort Order	See [Common fields](#)

Trusted Access

Trusted access enables specialized "ews" templates to be accessed externally without first having to login to Emerald. Uses of trusted access include presenting information to the public such as a qualification portal, remote calendaring, system monitoring and support for incoming IPN transactions from external platforms.



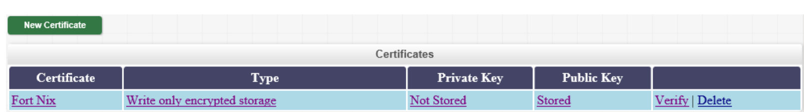
By default all trusted resources included with Emerald are inactive and can be activated as needed.



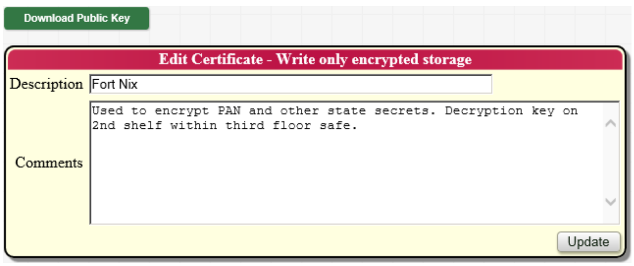
Field	Description
Resource Label	Short description of the purpose of the trusted resource
File Name	Filename of "ews" template to be treated as a trusted resource. This template must be specifically designed to be used as a trusted resource.
Run As	When ews template is called this determines operator group trusted resource is to be run as. This operator group is used regardless of whether user referencing the file is logged on to Emerald or not. If an operator is already logged on their session is ignored for the purpose of servicing requests for trusted resources. Operator group selection respects any IP access restrictions normally assigned to the selected group as well as all file, table, column and label based access controls associated with operator group. Each and every ews template has **unlimited access** to Emerald regardless of the operator group it runs as. There is no safe operator group that may possibly be configured to protect the system from a malicious or improperly designed ews template.
Description	Detailed information about this trusted resource including service it provides and any security or configuration requirements.
Comments	Additional information about this resource set by operators
Active	When "Yes" this trusted resource is reachable by anyone without authentication. When "No" resource is not reachable.

Certificates

Currently certificates manage public key encryption for stored data. In future versions of Emerald this menu provides a CA function for certificate provisioning.

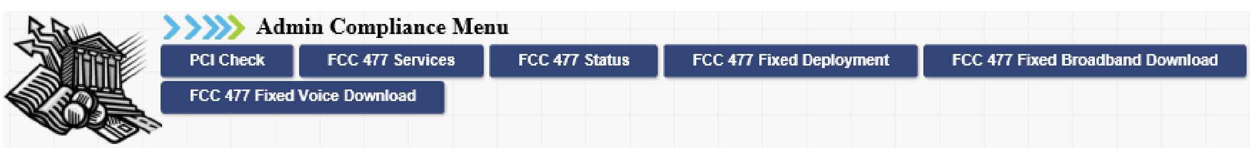


Field	Description
Certificate type	Determines usage and configuration of certificates to be generated. Please reference on screen description for information about each certificate type.
Keying options	When creating new certificates keying options manage whether existing certificates are to be imported or new certificates generated.
Key size	Key size appears when Emerald generates a new private key. Key length of 2048-bit is recommended. A key length of 4096-bit doubles storage required for encrypted data field.
Private key download	The private key download appears when Emerald generates a new private key that will not be stored within Emerald. When download link appears the key must be downloaded and stored in a safe location. There is no future opportunity to download the private key after certificate is created since the private key is never stored within Emerald database. Loss of private key results in loss of ability to decrypt encrypted data or perform signing operations.



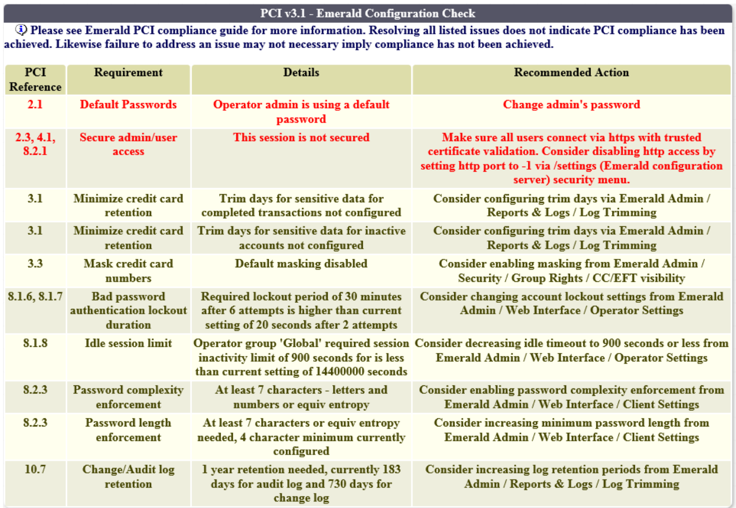
COMPLIANCE

Compliance offers operators assistance in meeting government/industry reporting and security requirements.



Worldwide - PCI Check

PCI check is intended to be used in conjunction with our PCI compliance document as a convenience to point out prescriptive PCI requirements able to be detected and addressed within the context of Emerald configuration. PCI check is not able to determine your organizations overall compliance with all PCI requirements. Items appearing in bright red indicate important configuration problems we recommend addressing as soon as possible.



PCI v3.1 - Emerald Configuration Check			
Please see Emerald PCI compliance guide for more information. Resolving all listed issues does not indicate PCI compliance has been achieved. Likewise failure to address an issue may not necessary imply compliance has not been achieved.			
PCI Reference	Requirement	Details	Recommended Action
2.1	Default Passwords	Operator admin is using a default password	Change admin's password
2.3, 4.1, 8.2.1	Secure admin/user access	This session is not secured	Make sure all users connect via https with trusted certificate validation. Consider disabling http access by setting http port to -1 via /settings (Emerald configuration server) security menu.
3.1	Minimize credit card retention	Trim days for sensitive data for completed transactions not configured	Consider configuring trim days via Emerald Admin / Reports & Logs / Log Trimming
3.1	Minimize credit card retention	Trim days for sensitive data for inactive accounts not configured	Consider configuring trim days via Emerald Admin / Reports & Logs / Log Trimming
3.3	Mask credit card numbers	Default masking disabled	Consider enabling masking from Emerald Admin / Security / Group Rights / CC/EFT visibility
8.1.6, 8.1.7	Bad password authentication lockout duration	Required lockout period of 30 minutes after 6 attempts is higher than current setting of 20 seconds after 2 attempts	Consider changing account lockout settings from Emerald Admin / Web Interface / Operator Settings
8.1.8	Idle session limit	Operator group 'Global' required session inactivity limit of 900 seconds for is less than current setting of 14400000 seconds	Consider decreasing idle timeout to 900 seconds or less from Emerald Admin / Web Interface / Operator Settings
8.2.3	Password complexity enforcement	At least 7 characters - letters and numbers or equiv entropy	Consider enabling password complexity enforcement from Emerald Admin / Web Interface / Client Settings
8.2.3	Password length enforcement	At least 7 characters or equiv entropy needed, 4 character minimum currently configured	Consider increasing minimum password length from Emerald Admin / Web Interface / Client Settings
10.7	Change/Audit log retention	1 year retention needed, currently 183 days for audit log and 730 days for change log	Consider increasing log retention periods from Emerald Admin / Reports & Logs / Log Trimming

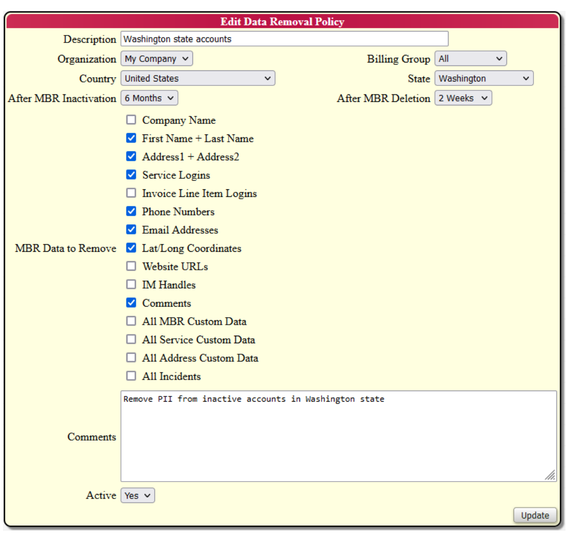
Worldwide - PII Retention

New Policy Status Check

PII Retention Policies

Description	Organization	Group	Country	State	Remove Data	Inactive MBRs	Deleted MBRs	
Washington state accounts	My Company	All	United States	Washington	• First Name + Last Name • Address1 + Address2 • Service Logins • Phone Numbers • Email Addresses • Lat/Long Coordinates • Comments • 1 x Account Custom Data • 3 x Incidents By Type	6 Months	2 Weeks	Delete

These settings focus on retention of PII (personally identifying information) once an MBR has been inactivated or deleted. Retention of security related information such as passwords or personal account numbers, change histories and other log data is managed separately from Emerald Admin / Reports & Logs / Log Trimming. File retention once MBRs have been inactivated can be found under Emerald Admin / General / File Categories. All data removal operations are nonreversible. Should multiple retention policies apply to an MBR the most permissive settings across all policies are applied.



Field	Description
Description	Unique informational text describing the PII entry

Organization	See Common fields
Billing Group	See Common fields
Country	Restricts the data removal policy to inactivated or deleted MBRs where the MBR level billing address is in the matching country. If one or more service addresses match the country while the MBR level billing address does not then PII removals are constrained to matching services and will not apply to MBR data or other services in the MBR whose service address does not have a matching country.
State	Further restricts data removal policy by state. See country above for details.
After MBR Inactivation	Duration from the later of the time the MBR was inactivated or last modified post inactivation to trigger PII removal. This setting applies exclusively to inactivated MBRs.
After MBR Deletion	Duration from the later of the time the MBR was deleted to trigger PII removal. This setting applies exclusively to deleted MBRs.
MBR Data to Remove	Determines information to be removed when checked. (See options table below.)
Comments	Related additional information
Active	When active the data removal policy is allowed to remove PII. When inactive the data removal policy will still reflect pending removals under "Status Check" however no data will be removed when the scheduled task "Trim PII" runs.

Option	Description
Company Name	Address level field
First + Last Name	Address level fields
Address1 and Address2	Address level fields
Service Logins	Service level field
Invoice Line Item Logins	Invoice line item field
Phone Numbers	Address level Home, Work, Fax and Mobile numbers
Email Addresses	Address and service level Email fields
Lat/Long Coordinates	Address level Latitude and Longitude as well as Geocoder synchronization data for the address.
Website URLs	Address level field
IM Handles	Address level field
Comments	MBR, service and address level comments fields
All MBR Custom Data	All MBR level custom data fields, to selectively remove certain custom data fields leave this setting unchecked and add Account Data fields below this form.
All Service Custom Data	All service level custom data fields, to selectively remove certain custom data fields leave this setting unchecked and add "Account Custom Data" fields below this form.
All Address Custom Data	All address level custom data fields, to selectively remove certain custom data fields leave this setting unchecked and add "Address Custom Data" fields below this form.
All Incidents	All incidents will be removed, to selectively remove certain incidents by incident type leave this setting unchecked and add "Incidents Of Type" fields below this form.

Status Check

Status check displays a summary of PII data to be removed the next time "Trim PII" scheduled task runs without changing any existing data. To drill down and get more detailed information about removals follow the hyperlink in the description field.

Return

Pending PII Removals

Description	Address Changes	Address Custom Data Removals	MBR Changes	MBR Custom Data Removals	Invoice Line Item Changes	Service Changes	Service Custom Data Removals	Incident Removals	Incident Custom Data Removals
Washington state accounts	3	0	3	1	0	3	0	0	0

If a PII retention policy has been inactivated its data still appears under Status Check even though its data will not be processed for removal the next time Trim PII scheduled task runs.

United States – FCC - Broadband Labels

For U.S. based Internet broadband providers required to display broadband labels at point of sale this menu enables creation and management of broadband labels. FCC's broadband labels are a generalization intended to provide customers with a high level summary and may not completely align with open ended nature of plans possible in Emerald. In this case additional important details about services, pricing and discounting not captured in the labels should be included within provider policy URLs.

Once necessary details have been entered both broadband labels and machine readable CSV can be exported from Emerald and incorporated into company storefronts and website or linked directly to Emerald for public access. Linking has the advantage of not having to download and distribute new versions as information changes.

Broadband labels are available from within manage account area of the customer center and account information area of signup form.

For more information about FCC broadband labels: https://www.fcc.gov/broadbandlabels

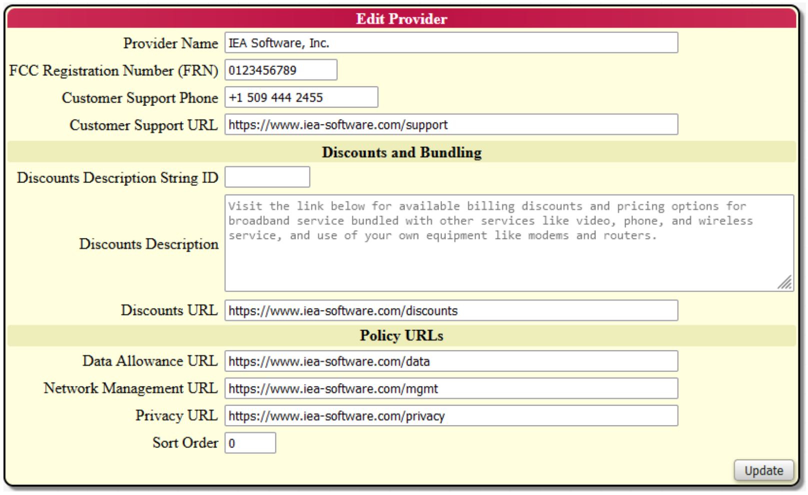
Providers

Providers maintain basic company information and references to required policy URLs. Multiple providers can be created with the same FCC FRN to apply a different set of policy URLs for residential vs. business customers within an organization.

New Provider | Providers | Contracts | Additional Charges | Service Types | Status | View Labels | Data Export

Providers

Provider Name	Registration Number	Support Phone	Support URL	Discounts URL	Data Policy URL	Management Policy URL	Privacy Policy URL	
IEA Software, Inc.	0123456789	+1 509 444 2455	https://www.iea-software.com/support	https://www.iea-software.com/discounts	https://www.iea-software.com/data	https://www.iea-software.com/mgmt	https://www.iea-software.com/privacy	Delete



Field	Description
Provider name	Company name to appear on the broadband label.
FCC Registration Number (FRN)	10-digit FCC assigned registration number. FRN forms the first 10 digits of the unique plan identifier presented on the broadband label.
Customer Support Phone	Displayed in the customer support section of the broadband label.
Customer Support URL	Displayed within customer support section of the broadband label. URLs should be kept short for printed display.
Discounts Description String ID	See Common fields
Discounts Description	Brief overview of what is covered within Discounts URL appearing within discounts area of the broadband label. If description is left blank default FCC discount text is used. Should both 'Discounts Description' and 'Discounts URL' be left blank the discounts area is omitted from the broadband label.
Data Allowance URL	Optional URL further explaining any data limits and overages. If left blank the URL is omitted from the broadband label. URLs should be kept short for printed display.
Network Management URL	Link to network management policies such as queue management, security, blocking, throttling and paid prioritization. URLs should be kept short for printed display.
Privacy URL	Link to privacy policy. URLs should be kept short for printed display.
Sort Order	See Common fields

Contracts

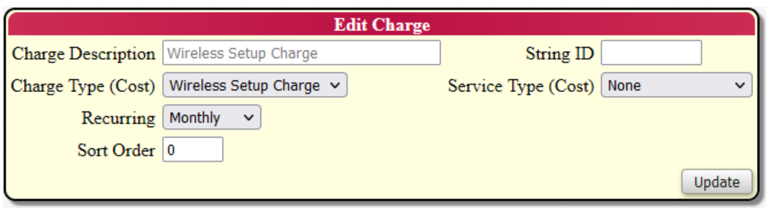
Manages contract related information appearing on the broadband label.

Field	Description

Description	Unique description of the contract. This field is not displayed on broadband label.
Contract Terms URL	Link to terms of contract. If omitted field is omitted from broadband label. URLs should be kept short for printed display.
Contract Required	Whether or not contract is required for service.
Contract Months	Length of contract in months.
Early Termination Fee	Fee for early termination, if variable include maximum amount and additional information within contract terms URL.
Sort Order	See [Common fields]

Additional Charges

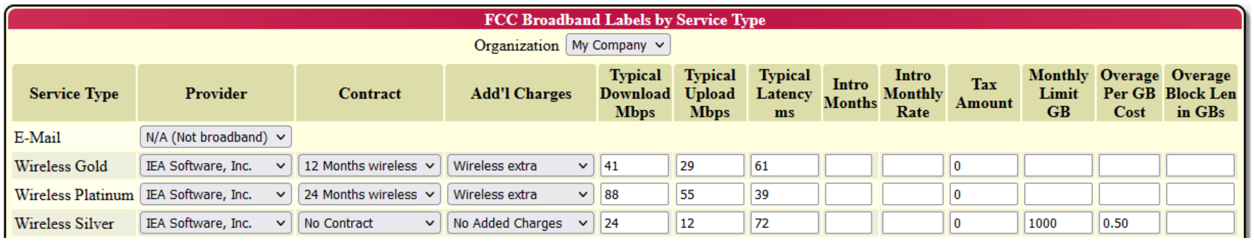
Itemize extra one time and recurring fees **excluding normal service types monthly cost and setup fees defined within service type configuration.** If it is customary to charge additional one time and recurring fees (e.g. equipment rentals, cost recovery fees, added service charges, professional install fees, late fees) beyond service type cost and setup charge(s) add them here.



Field	Description
Charge Description	If a charge type or service type is selected charge description can be left blank to use description from referenced selection. If specified charge description overrides service type or charge type description. If no charge type or service type is selected the charge description field is required.
String ID	See [Common fields]
Charge Type (Cost)	When selected cost is derived from corresponding charge type.
Service Type (Cost)	When selected cost is derived from corresponding service type.
Charge Discount (Cost)	When selected cost is derived from corresponding discount. Only discounts of type 'Charge – Percentage' and 'Charge – Static Amount' are applicable.
Recurring	Indicates whether the charge is a monthly recurring fee or one-time cost.
Cost	When both service and charge types are set None the cost field allows a custom price to be defined.
Sort Order	See [Common fields]

Service Types

At the organization level per service type details appearing on the broadband label such as providers and typical speeds are managed from this menu. Before managing service types providers, contracts and additional charges should first be defined. Service types having not been previously managed from this menu are sequenced first and appear with a green background. If managing multiple organizations it is important to update the form first before switching to another organization as all unsaved changes are lost when switching.



FCC Broadband Labels by Service Type

Organization: My Company

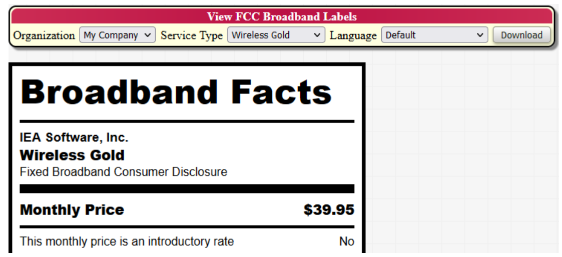
Service Type	Provider	Contract	Add'l Charges	Typical Download Mbps	Typical Upload Mbps	Typical Latency ms	Intro Months	Intro Monthly Rate	Tax Amount	Monthly Limit GB	Overage Per GB Cost	Overage Block Len in GBs
E-Mail	N/A (Not broadband)											
Wireless Gold	IEA Software, Inc.	12 Months wireless	Wireless extra	41	29	61			0			
Wireless Platinum	IEA Software, Inc.	24 Months wireless	Wireless extra	88	55	39			0			
Wireless Silver	IEA Software, Inc.	No Contract	No Added Charges	24	12	72			0	1000	0.50	

Field	Description
Provider	Determines company information and policy URLs applicable to the service type. When provider is N/A service type is not a broadband service subject to broadband labeling. Available providers are managed from providers menu above.
Contract	References any contract terms that may be applicable to new customers. Available contracts are managed from contracts menu above.
Add'l Charges	Set of additional one time and recurring fees applicable to new customers who receive this service beyond included services monthly cost and service type setup fees. Available charges are managed from additional charges menu above.
Typical Download Mbps	Typical download speed may differ from advertised or provisioned speeds in that it represents the speed customer would generally be measured to receive. This field does not reflect either lowest speed during peak usage or highest speed during low usage. By default bandwidth values from FCC services form is set in this field for reference purposes and may have to be modified as FCC services reflect advertised rather than typical speed.
Typical Upload Mbps	Typical upload speed may differ from advertised or provisioned speeds in that it represents the speed customer would generally be measured to receive. This field does not reflect either lowest speed during peak usage or highest speed during low usage. By default bandwidth values from FCC services form is set in this field for reference purposes and may have to be modified as FCC services reflect advertised rather than typical speed.
Typical Latency ms	Typical round trip latency in milliseconds the customer would generally receive.
Intro Months Intro Monthly Rate	If an introductory period applies to this service for new customers enter both length of the period and monthly rate or leave both fields blank if no introductory period is available.
Tax Amount	Total cost of all monthly government imposed taxes on this service. If there are none enter 0, if rate varies / can't generally be determined leave the field blank and the government taxes line item in the broadband label will show tax varies.
Monthly Limit GB	Monthly data limit in gigabytes. If there is no monthly limit leave this field blank.
Overage Per GB Cost	Once monthly limit is reached the per-gigabyte cost of additional data. If there is no monthly limit or additional data cannot be purchased leave this field blank.
Overage Block Len in GBs	The minimum size data block that can be purchased or charged for overages. For example once the monthly limit of 1000 GB is reached customer must purchase an additional block of 20 GB at a cost of $10. In this case 'Overage Per GB Cost' is 0.50 and 'Overage Block Len in GBs' is 20. If block purchases or charges greater than 1 GB are not required this field should be left blank.

Status

Checks broadband labels associated with selected organization for missing data or known configuration problems.

View Labels



View or download FCC broadband labels for embedding into a company website.

Optionally once enabled this interface provides publically accessible URLs to current version of a selected broadband label. URLs are then linked or embed into company site to avoid manually downloading new labels as information such as pricing changes.

To enable public access to broadband labels activate trusted resource "FCC Broadband Label - View Label" from Emerald Admin / Security / Trusted Access.

Data Export

Download machine readable CSV export of organizations broadband labels to make CSV data available from a company website. Optionally once enabled this interface provides publically accessible URLs to an organizations current broadband labels in machine readable form. URLs are then linked from company site to avoid having to download new CSV files as label data changes.

To enable public access to broadband labels activate trusted resource "FCC Broadband Label - Data Export" from Emerald Admin / Security / Trusted Access.

For description of machine readable data fields in the CSV file:

https://www.fcc.gov/sites/default/files/broadband-label-machine-readable-file-data-specifications.pdf

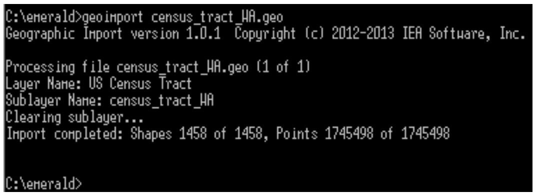
United States – FCC - BDC Subscriptions

For U.S. based Internet broadband and VoIP providers required to submit Broadband Data Collection (BDC) Emerald offers a set of features to automate **broadband subscriptions** reporting. Information related to **broadband deployment** representing your service area is not currently stored in Emerald and must be reported based on your coverage maps following FCC provided instructions.

Begin by downloading US census geographic datasets for all US states and territories you currently provide covered broadband and VoIP services from our website:

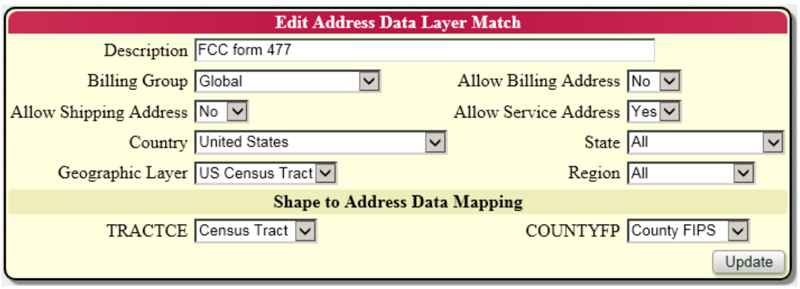
https://www.iea-software.com/ftp/EmeraldV6/Geography/North_America/United_States/Census/

Unzip files and run geoimport utility located in Emerald folder followed by name of uncompressed ".geo" file. (E.g. geoimport census_tract_WA.geo) You may call geoimport for each file individually or use wildcard such as *.geo to batch import all files at once.



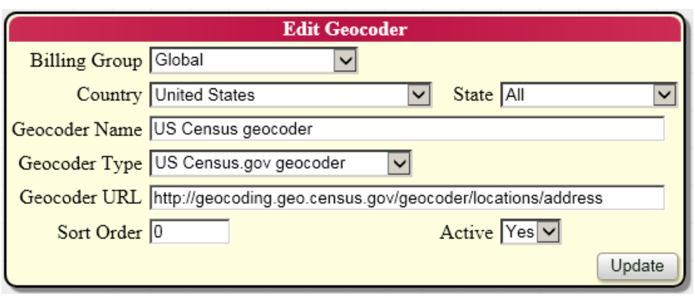
When the import process has completed configure [address custom data synchronization](#) (Emerald Admin / Geography / Address Layer Data) for the "US Census Tract" layer mapping address custom data field "Census Tract" to TRACTCE and "County FIPS" to COUNTYFP per screenshot below.

Please check [scheduler](#) to confirm scheduled task "Geographic match address coordinates by layer" is activated.



Configure one or more [geocoders](#) (Emerald Admin / Geography / Geocoders) to determine latitude and longitude of each service address. Alternately location data may be entered manually for a service address by enabling the "Coordinates" field for each [address type](#) (Emerald Admin / Geography / Address Types).

Please check [scheduler](#) to confirm the schedule task "Geocode accounts with new or updated address information" is activated.



Finally completely configure [FCC technology to service type mappings](#) (Emerald Admin / Compliance / FCC Services).

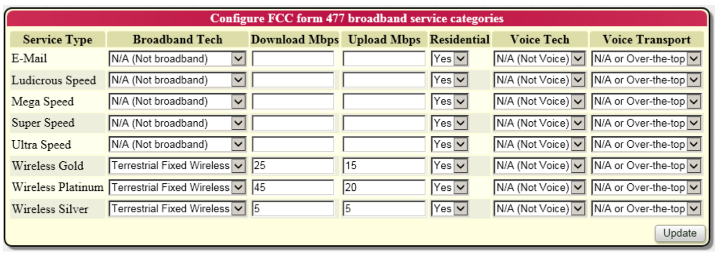
It will normally take some number of hours for the geocoder and geographic query scheduled tasks to execute initially given their default run intervals. If you would prefer to have data processed right away without this delay click "Process" option for your geocoder(s) (Emerald Admin / Geography / Geocoders) Once geocoding has fully completed then logged on as an administrator browse to /geoproc.ews (e.g. https://myemeraldserver/geoproc.ews) This will run geographic queries to determine census tract and county FIPS for each service address.

Before submitting any data it is important to review FCC status report and address any problems reported. It is often the case initially there may be a number of addresses (such as PO boxes) which cannot be geocoded automatically. Manual action is required to obtain either physical address or latitude and longitude coordinates in these cases.

Once any reported problems are resolved relevant data may be exported for upload to FCC website. Please see sections below for more information.

FCC Services

Mapping between FCC technology for BDC reporting and Emerald service types is configured within this menu. If a service type is not a covered broadband or VoIP service select "N/A". Please see FCC documentation for more information about selection of specific technologies and transports. Download and Upload rates should match advertised rather than typical or actual rates.

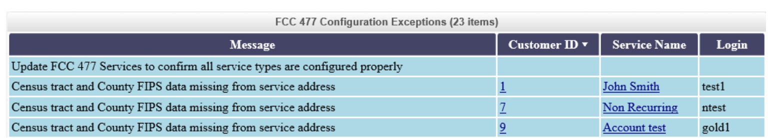

Configure FCC form 477 broadband service categories

Service Type	Broadband Tech	Download Mbps	Upload Mbps	Residential	Voice Tech	Voice Transport
E-Mail	N/A (Not broadband)			Yes	N/A (Not Voice)	N/A or Over-the-top
Ludicrous Speed	N/A (Not broadband)			Yes	N/A (Not Voice)	N/A or Over-the-top
Mega Speed	N/A (Not broadband)			Yes	N/A (Not Voice)	N/A or Over-the-top
Super Speed	N/A (Not broadband)			Yes	N/A (Not Voice)	N/A or Over-the-top
Ultra Speed	N/A (Not broadband)			Yes	N/A (Not Voice)	N/A or Over-the-top
Wireless Gold	Terrestrial Fixed Wireless	25	15	Yes	N/A (Not Voice)	N/A or Over-the-top
Wireless Platinum	Terrestrial Fixed Wireless	45	20	Yes	N/A (Not Voice)	N/A or Over-the-top
Wireless Silver	Terrestrial Fixed Wireless	5	5	Yes	N/A (Not Voice)	N/A or Over-the-top

Update

FCC Status

Status provides an overview of overall state of BDC data including any detected configuration problems or missing data that might result in inaccurate or incomplete reporting. It is recommended this menu be checked and all listed exceptions resolved prior to submitting data to FCC.


FCC 477 Configuration Exceptions (23 items)

Message	Customer ID ▾	Service Name	Login
Update FCC 477 Services to confirm all service types are configured properly			
Census tract and County FIPS data missing from service address	1	John Smith	test1
Census tract and County FIPS data missing from service address	7	Non Recurring	ntest
Census tract and County FIPS data missing from service address	9	Account test	gold1

FCC Fixed Broadband Subscription Download

This menu option downloads CSV file of fixed broadband subscriptions (FBS) for upload to FCC web portal. It is recommended exception report within FCC status menu be checked for any problems prior to uploading data to FCC portal.

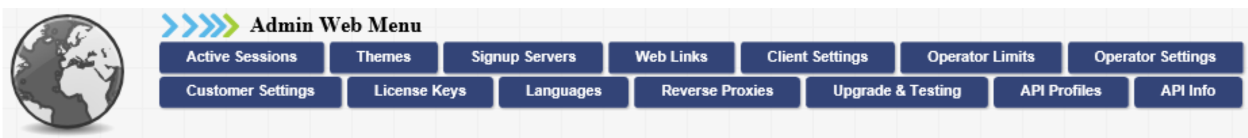
When filing is set to Broadband Data Collection (BDC) subscription data is downloaded according to BDC specific technology code groupings. Before downloading it is recommended operators check to make sure under FCC Services best matching broadband technology code is selected.

FCC Fixed Voice Download

This menu option downloads CSV file of fixed voice service (FVS) for upload to FCC web portal. It is recommended exception report within FCC status menu be checked for any problems prior to uploading data to FCC portal.

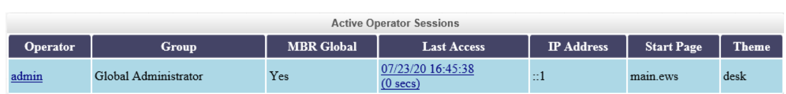
WEB INTERFACE

Configuration of web interface related settings including: View and remove active operator sessions, theme and signup server setup, hyperlinks, client settings and search limits, license keys, language translations, reverse proxy configuration and upgrade & test safing.



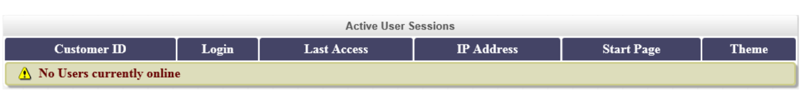
Active Sessions

All operators and customers currently logged into emerald are visible from Active session's menu. Clicking "Operator" field allows editing of configuration of that operator. Clicking "Last Access" field disconnects an active operator forcing the operator to re-authenticate. Source IP address displayed is based on IP observed from this client's last access. If operator is logged on at same time on different systems or network address changes during the course of a login session IP address displayed is updated. Active sessions are local to each Emerald server. If multiple Emerald servers are used for redundancy different sessions may be active on each server.



Active Operator Sessions

Operator	Group	MBR Global	Last Access	IP Address	Start Page	Theme
admin	Global Administrator	Yes	07/23/20 16:45:38 (0 secs)	::1	main.ews	desk

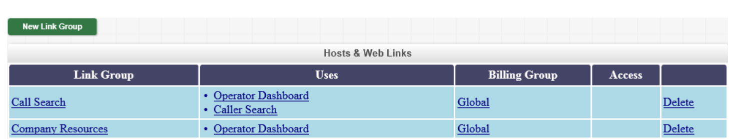


Active User Sessions

Customer ID	Login	Last Access	IP Address	Start Page	Theme
No Users currently online					

Web Links

Web links provide hyperlink for resources and intranet applications within operator dashboard, host monitoring dashboard, address physical location linking, customer account center and

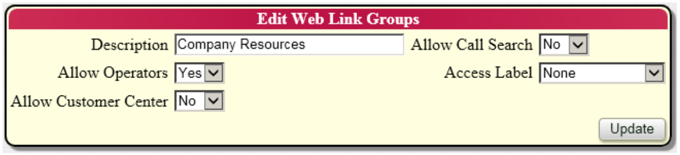


New Link Group

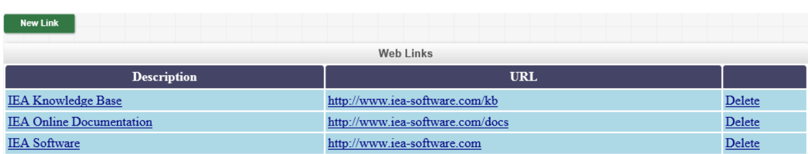
Hosts & Web Links

Link Group	Uses	Billing Group	Access	
Call Search	• Operator Dashboard • Caller Search	Global		Delete
Company Resources	• Operator Dashboard	Global		Delete

Caller-ID popup software.   Links are organized into groups which control access and specify where links within the group may be used.



Field	Description
Description	Unique label for this link group. Link groups are selectable when adding links to the operator dashboard.
Operator Pinger	When select the link group contains a list of hosts available to the 'host ping monitor' operator dashboard.
Address Coordinates	When selected the link group is used for hyperlinking address latitude and longitude coordinates within Show MBR and Service menus of Emerald client to external mapping services. Follow on-screen instructions when adding a hyperlink for help formatting URL to interface with external service. Only a single link can be referenced per MBR. Additional links are ignored.
Allow Call Search	Allow links within this group to appear as Caller-ID lookup helpers in the Emerald caller id popup application.
Allow Operators	Allow this group to be selectable by operators when managing their dashboard
Access Label	See Common fields
Allow Customer Center	Allow links within this group to appear in the customer account center



New Link

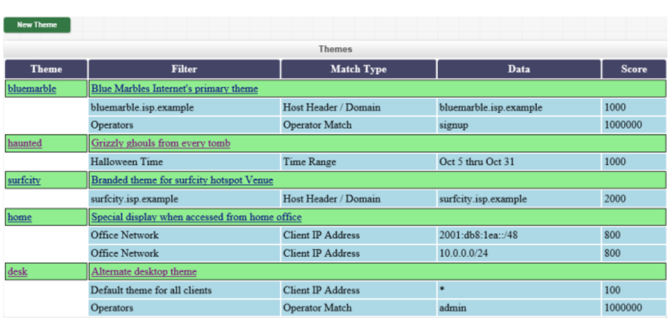
Web Links

Description	URL	
IEA Knowledge Base	http://www.iea-software.com/kb	Delete
IEA Online Documentation	http://www.iea-software.com/docs	Delete
IEA Software	http://www.iea-software.com	Delete

Once a group is created one or more web links can be assigned to the group. When creating a link for Caller-ID lookup application phone number is appended to the end of the hyperlink.

Themes

The ability to customize Emerald interface has several important benefits. Resellers can tailor Emerald to more closely match an existing web site or include company logos and designs. Hotspot operators can have the appearance of a unique presence in multiple venues without separate hardware or software. Layouts designed for vastly different form factors open new possibilities for service management.



New Theme

Themes

Theme	Filter	Match Type	Data	Score
bluemarble	Blue Marbles Internet's primary theme			
	bluemarble.isp.example	Host Header / Domain	bluemarble.isp.example	1000
	Operators	Operator Match	signup	1000000
haunted	Grizzly ghouls from every tomb			
	Halloween Time	Time Range	Oct 5 thru Oct 31	1000
surfcity	Branded theme for surfcity hotspot Venue			
	surfcity.isp.example	Host Header / Domain	surfcity.isp.example	2000
home	Special display when accessed from home office			
	Office Network	Client IP Address	2001:db8:1ea::/48	800
	Office Network	Client IP Address	10.0.0.0/24	800
desk	Alternate desktop theme			
	Default theme for all clients	Client IP Address	*	100
	Operators	Operator Match	admin	1000000

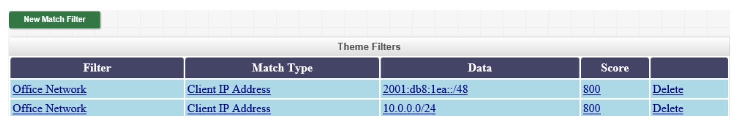
Themes are based on two technologies: Cascading Style Sheets (CSS3) and a theme folder inheritance system unique to Emerald. Working together themes can range from changing colors or logos to designing a completely new look and feel. References for CSS3 are available from W3C http://www.w3.org/Style/CSS/ and folder inheritance system is described in detail below.

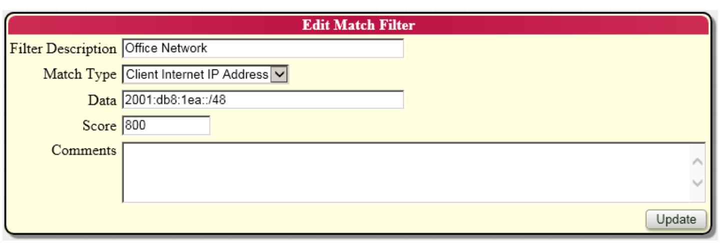
For each web request to Emerald information such as Operator, client IP address, host header, time, browser type and others are examined and scored based on the rules configured for each theme. After all rules are examined the theme having the highest score is used in rendering the web interface.

Field	Description
Theme	Short theme name which matches subdirectory name of the Emerald theme folder (Emerald/web/themes/mytheme) on Emerald server where files specific to this theme are located. Only themes containing characters a-z, 0-9 and _ are accepted.
Description	Text showing the purpose and any useful notes for this theme. Description field is informational and only displayed here.

Theme Filters

Scores are awarded to themes having "theme filters" which match a set criterion. Each matching theme filter adds its score value to that themes total. The theme having highest score is used.





Field	Description
Filter Description	Text describing the purpose of the filter
Match Type	Reflects source and type of data being matched. The following match types are currently available. **Match Type** | **Description**

	Host Header / Domain	Matches host header (HTTP_HOST) of incoming web request. This is the DNS name entered into URL bar of the browser. Commonly used to specify primary theme displayed when users browse to primary URL. When using multiple TLS certificates, wildcard certs or subject alternate names a single instance of Emerald can present different themes based on entered URL.
	User Agent	Performs a substring match of user agent (HTTP_USER_AGENT) transmitted by client browser. Often used to target specialized themes at specific browsers or devices.
	Client IP Address	Matches IPv4 or IPv6 address of incoming requests from clients. Matching may be by IP address, subnet in CIDR form or DNS name.
	Time Range	Matches current time and date. See Common fields for information on format of time range.
Data	Value to match based on selected match type above	
Score	Relative theme score to add to themes total when "Data" matches "Match Type" condition.	
Comments	Additional information related to use of this filter.	

Theme Folders

All themes related information is stored on disk on Emerald server in web/themes subdirectory where Emerald is installed. Default theme included with Emerald is located in the "default" subfolder. Other user-created themes are located in subdirectory of web/themes corresponding to theme name. Any requested files from a subdirectory other than "default" are first looked for in that subdirectory. If file does not exist Emerald automatically looks for the same file in the "default" folder. This allows for the creation of new themes with minimal changes from the default without having to copy all files from the default folder into each theme folder. This approach has the added advantage in that themes are more likely to continue to work seamlessly in the face of new features and updates to the Emerald software.

When creating new themes copy only those files you will be changing. **Never make changes to files within the "default" theme** as any changes to default folder are overwritten when Emerald updates are installed. Additionally IEA produced or IEA reviewed third party themes may depend on facets of the default theme.

Themes should only be sourced from trusted parties as "ews" templates located in the theme folder have full access to Emerald database. See Emerald Web Extensions guide for more information on ".ews" template files.

When developing custom themes the following steps are recommended to maximize compatibility:

- Copy only files from default folder you wish to customize.
- Avoid customization of css_main.css and css_cust.css. Instead aspects of default theme can be customized by applying style changes to css_main_custom.css or css_cust_custom.css.
- Begin with theme examples available from https://www.iea-software.com/themes

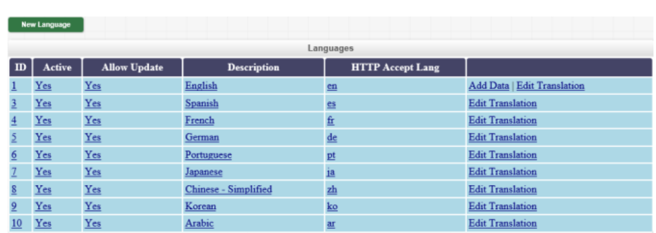
Following theme files are located in the "default" themes folder.

Theme File	File Description

css_cust.css	Emerald style sheet covering the Emerald Signup Server and Customer Account Center.
css_cust_custom.css	Emerald custom style sheet covering the Emerald Signup Server and customer Account Center. The custom style sheet is loaded after css_cust.css therefore styles defined in this file take precedence over similarly scoped classes in css_cust.css
css_main.css	Main Emerald style sheet covering the Emerald Client and Emerald Admin interfaces.
css_main_custom.css	Custom Emerald style sheet covering the Emerald Client and Emerald Admin interfaces. The custom style sheet is loaded after css_main.css therefore styles defined in this file take precedence over similar scoped classes in css_main.css
buttons_admin.ews	Renders top level set of Admin menu options
buttons_admin_sub.ews	Renders all sub level set of Admin menu options
buttons_billing.ews	Renders Emerald client billing menu options
buttons_cust.ews	Renders top level customer account center menu options
buttons_custset.ews	Renders service level options within manage account menu of customer center
buttons_file.ews	Renders options for MBR and service level file attachments
buttons_history.ews	Renders MBR account history menu options
buttons_incident.ews	Renders MBR/Service incident menu options
buttons_infobar.ews	Renders Information bar above main menu
buttons_inv.ews	Renders Inventory menu options from main menu of Emerald client
buttons_invoice.ews	Renders MBR invoice menu options
buttons_main.ews	Renders top level Emerald client menu options
buttons_mareport.ews	Renders MBR level reporting menu including MBR level custom reports
buttons_mbr.ews	Renders MBR level menu options
buttons_payment.ews	Renders MBR level payments menu options
buttons_pref.ews	Renders operator preferences menu of Emerald client
buttons_report.ews	Renders Reporting menu options
buttons_sa.ews	Renders MBR Service menu options
buttons_sareport.ews	Renders service level reporting menu including service level custom reports
buttons_search.ews	Renders Emerald client search menu options
buttons_statement.ews	Renders MBR statement menu options
buttons_support.ews	Renders Emerald client support menu options
buttons_timeline.ews	Renders MBR and service level timeline menu options
custom_admin_header.ews	Allows custom inclusion of additional information in the Emerald admin header before the top level menu options.
custom_cust_cc.ews	Allows custom inclusion of additional information in the payment form when making one time CC payments from Customer Account Center.
custom_cust_ccauto.ews	Allow custom inclusion of additional information within payment form when entering CC for recurring automatic payments from Customer Account Center.
custom_cust_eft.ews	Allows custom inclusion of additional information in the payment form when making one time EFT payments from Customer Account Center.
custom_cust_footer.ews	Allows custom inclusion of additional information in the footer class of the Customer Account Center.
custom_cust_header.ews	Allows custom inclusion of additional information in the header of the Customer Account Center before the top level menu options.
custom_cust_status.ews	Allows custom inclusions of additional information in the Account Status display of the Customer Account Center after all internal status fields are displayed.
custom_main_header.ews	Allows custom inclusion of additional information in the header of the Emerald Client main menu before the main menu options.
custom_mbr_aftermenu.ews	Allows custom inclusion of additional information in the MBR header after the MBR menu options.
custom_mbr_edit.ews	Allows custom inclusion of additional information in the MBR edit form. *

custom_mbr_header.ews	Allows custom inclusion of additional information in the MBR header before the MBR menu options.
custom_mbr_save.ews	Allows custom inclusion of additional information within the MBR save transaction when saving changes to an MBR.
custom_sa_aftermenu.ews	Allows custom inclusion of additional information in the MBR Service after the service menu options.
custom_sa_edit.ews	Allows custom inclusion of additional information within the Service edit form after the custom data dialogues.
custom_sa_header.ews	Allows custom inclusion of additional information in the MBR Service before the service menu options.
custom_sa_save.ews	Allows custom inclusion of additional information when saving an MBR Service after the save transaction has completed.
custom_signup_footer.ews	Allows custom inclusion of additional information in the footer of the Signup server
custom_signup_header.ews	Allows custom inclusion of additional information in the header of the Signup server
custom_signup_contact.ews	Allows custom inclusion of additional information in the contact form of the signup server after the login and password fields.
custom_signup_pay.ews	Allows custom inclusion of additional information in the payment form of the signup server after the pay method specific fields are displayed
menu_detail_mbr.ews	When showing MBR detail in the Emerald client this glues together information from various sources.
menu_detail_pkg.ews	When showing MBR package detail in the Emerald client this glues together information from various sources.
menu_detail_sa.ews	When showing MBR Service in the Emerald client this glues together information from various sources.
signup_done.ews	Called after the customer signup process has completed successfully.
signup_intro.ews	When customer first accesses the signup server this menu is loaded first which provides an introduction, EULA…etc. When finished the intro should link to signup_package.ews to begin the signup process.
signup_progress.ews	When using the signup server signup_progress.ews is responsible for displaying the progress bar at the top of the screen.
_login.ews	Displays the initial Emerald Login/Password screen when accessing Emerald. Note the _ character in _login.ews instructs Emerald not to enforce operator file security checking on the file.
quickreport_header.ews	Displays heading of quick reports including display of company logo and search parameters selected when executing quick report. This theme file is used by quick custom reports within the reports menu as well as MBR and service level reports menus when report output format is "display report"
quickreport_footer.ews	Display quick report footer after quickreport_header.ews and all report specific output has been displayed.

Languages



New Language

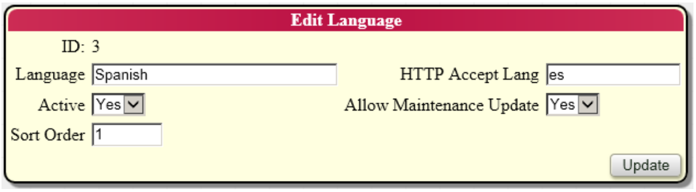
Languages

ID	Active	Allow Update	Description	HTTP Accept Lang	
1	Yes	Yes	English	en	Add Data | Edit Translation
3	Yes	Yes	Spanish	es	Edit Translation
4	Yes	Yes	French	fr	Edit Translation
5	Yes	Yes	German	de	Edit Translation
6	Yes	Yes	Portuguese	pt	Edit Translation
7	Yes	Yes	Japanese	ja	Edit Translation
8	Yes	Yes	Chinese - Simplified	zh	Edit Translation
9	Yes	Yes	Korean	ko	Edit Translation
10	Yes	Yes	Arabic	ar	Edit Translation

Emerald Client, Customer Access Center and Signup Servers support for multiple languages is managed by translations configured through languages menu. Generally selection of best language for the operator is chosen automatically based on web browser's language configuration. If a translation for browser's first language choice is not available Emerald falls back to using subsequent backup languages configured in the browser. If there are no language matches English language is used. Emerald operators can override language auto detection from the Operator preferences menu in Emerald client.

Many translations provided with Emerald are more or less automated machine translations from US English. We welcome feedback from those with the resources to improve upon default translations provided with Emerald.

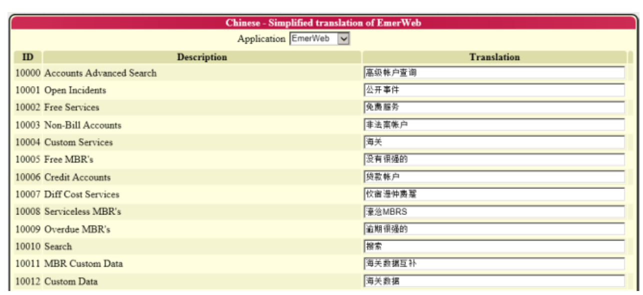
Use the "Add Data" link on the English language row to add additional StringIDs to support localization of custom additions to Emerald or add language support to items such as Service and Charge Types.



Field	Description
ID	Internal language Identifier. If providing a translation for an established language not specified please contact IEA Software support to reserve a language identifier for this language. If providing a translation for internal purposes (Customizing fields etc.) You must choose an ID starting above 10000.
Language	Name of the language or dialect in English
Active	When "Yes" language is loaded at startup and available to be used.
Allow String Updates	When "Yes" Emerald software updates automatically update translation for this language overwriting any custom changes to existing string translations. When "No" translation corrections are not applied as a result of future Emerald software updates. If you have customized or corrected a translation choose "No" to prevent your changes from being overwritten next time Emerald software is updated.
HTTP Accept Language	Language abbreviation used to match with browser selected languages
Sort Order	See [Common fields]

Editing Translations

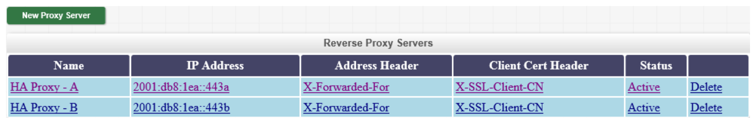
To edit an existing translation or create a translation for newly added language select "Edit Translation" option from the language listing above. The translation process is fairly straightforward. String ID and English description of strings is found on left while translation for the item is entered in translation box on the right. When finished updating or adding a translation click "Update" button at the very bottom of the translation form.



In order for changes to translations to take effect Emerald Web Server service / process must be restarted. "Apply" button within "Emerald Admin" cannot reload language data. To assist with the translation process a special debug option "Language Debug" is available within Emerald configuration server (/settings URL) under "Debug options". This setting enables language debugging whereby for each string of text displayed internal StringID of that text is shown throughout web interface.

```
When designing new or extensively editing an existing translation please take
care not to exceed your logon sessions idle timeout.  It is recommended
progress be periodically saved to limit possibility of losing translation
data.
```

Reverse Proxies

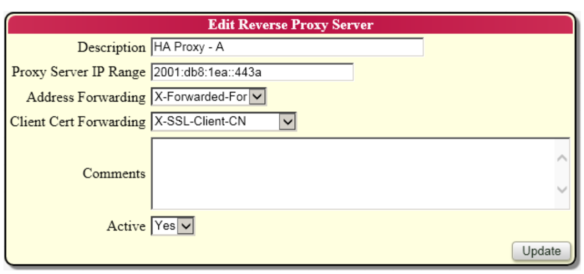

New Proxy Server

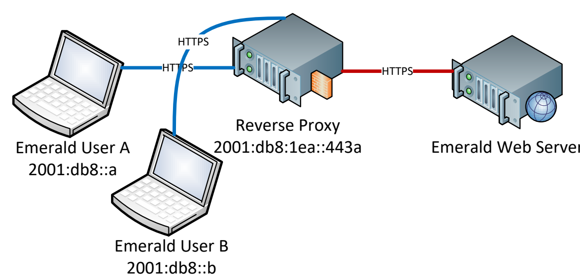
Reverse Proxy Servers

Name	IP Address	Address Header	Client Cert Header	Status	
HA Proxy - A	2001:db8:1ea::443a	X-Forwarded-For	X-SSL-Client-CN	Active	Delete
HA Proxy - B	2001:db8:1ea::443b	X-Forwarded-For	X-SSL-Client-CN	Active	Delete

Reverse proxies are front end proxy servers receiving requests from clients on behalf of a backend web server. They are typically used for high availability, load balancing, filtering and logging. Support for reverse proxies not operating in a "transparent" mode is configured in this menu. If using a reverse proxy please note the following:

- Two-factor certificate based authentication requires installing client auth CA public key into the reverse proxy and proxy configured to transmit X-SSL-Client-CN or X-SSL-Client-DN request headers. To prevent certificate authentication bypass proxies must be configured not to forward X-SSL-Client-CN or X-SSL-Client-DN headers from clients to Emerald. Connections between Emerald and forward proxy must be effectively protected against address spoofing.
- Reverse proxies should not be used with Emerald for the purpose of "load balancing" as this only increases load on backend database.
- Proxy must not cache or alter content or Emerald will not operate properly.





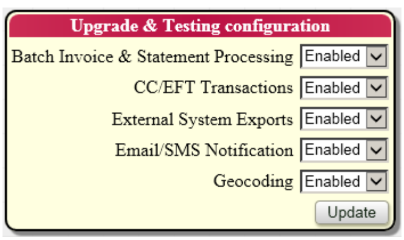
Field	Description
Description	Unique name for this reverse proxy server.
Proxy Server IP Range	Source IP address or address range of incoming requests from this proxy server. Once configured Emerald treats all requests from source address as proxy requests. HTTP requests from configured source IP or range are required to transmit proper address forwarding headers otherwise requests from source addresses fail.
Address Forwarding	Proxy header format to be used for passing original source address of the client as seen by the front end reverse proxy server. Forwarded address is used normally for enforcement of IP access controls and change audit logging. Reverse proxy servers are required to support one of the available standard address forwarding headers. If none of the formats are supported a reverse proxy entry for this proxy server must not be configured.
Client Cert	Header format used when forwarding client certificate identity for multifactor operator

Forwarding	authentication and TLS is terminated within reverse proxy. If enabled care should be taken to prevent this header from being forwarded by clients. Header must only be transmitted upon successful client certificate authentication by reverse proxy. Similarly opportunities for address spoofing should be mitigated to guard against client authentication bypass.
Comments	Additional information about this proxy server.
Active	When "Yes" all incoming requests from proxy IP address are treated as proxy requests. When "No" incoming requests from proxy IP are treated as normal requests from client browsers.

Upgrade & Testing

Upgrade & Test offers safing options to prevent unexpected scheduled or manual external transaction processing or notification. This feature may be useful during upgrades from Emerald version 5, database server migrations or when using Emerald in a test environment. By default after Emerald is upgraded from version 5 all settings are initially "Disabled".

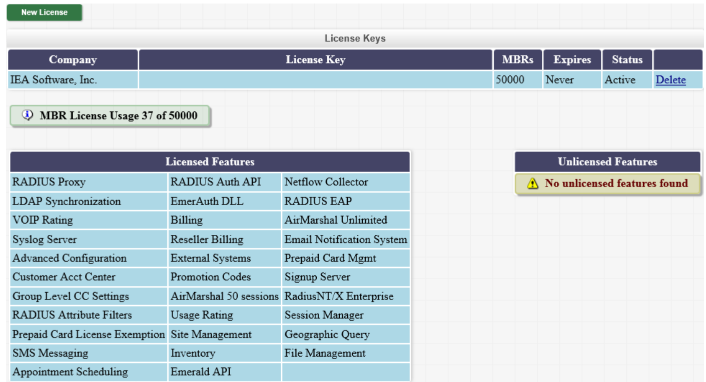
Disabling a feature does not cancel execution if related tasks are already running however all new instances of tasks are prevented from starting. Changes to Upgrade & Testing take effect immediately once updated and do not require clicking "Emerald Admin" / "Apply".



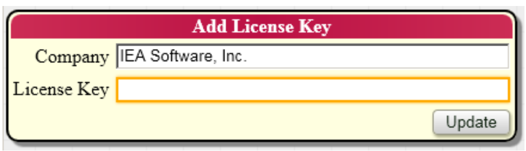
Field	Description
Batch Invoice & Statement Processing	When "Disabled" all invoice and statement batch level creation including Emerald Client / Billing menu and invoice or statement scheduled tasks are disabled. With this setting disabled batch level invoice and statement previews are still allowed as well as manual invoice and statement creation within each MBR.
CC/EFT Transactions	When "Disabled" all Credit Card and EFT all transaction processing is suspended. During this time transactions may continue to be queued for processing however no transactions are submitted to external CC/EFT gateways for processing..
External System Exports	When "Disabled" all external system synchronization from the Emerald export system (file exports and web service provisioning) is suspended. Sync / Export is also suspended. This does not include any systems that synchronize directly from the Emerald database or use Emerdap for LDAP synchronization.
Email/SMS Notification	When "Disabled" all Email and SMS notification is disabled. This includes subsystems which use notices including bulk email and batch sending of invoices and statements.
Geocoding	When "Disabled" all address geocoding including manual and automatic scheduled processing is suspended.

License Keys

Once Emerald database is created next step is registering your license keys within Emerald's license manager to begin using Emerald.



To begin login to Emerald with an admin account and follow license link displayed on screen or navigate to "Emerald Admin" / "Web Interface" / "License Keys" adding license key(s) you were provided. Most changes to license settings take effect immediately as license keys are updated.

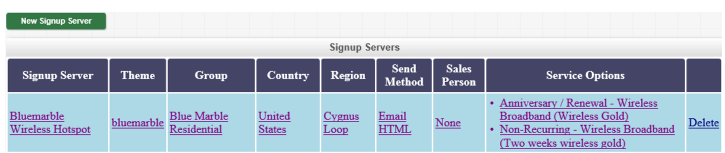


When you purchase or evaluate Emerald or add additional MBRs and feature, you will receive an Email with your License information. Enter exact Company Name and License Key that you receive in the E-mail. All spacing, punctuation and letter case must be entered exactly as shown in the license email.

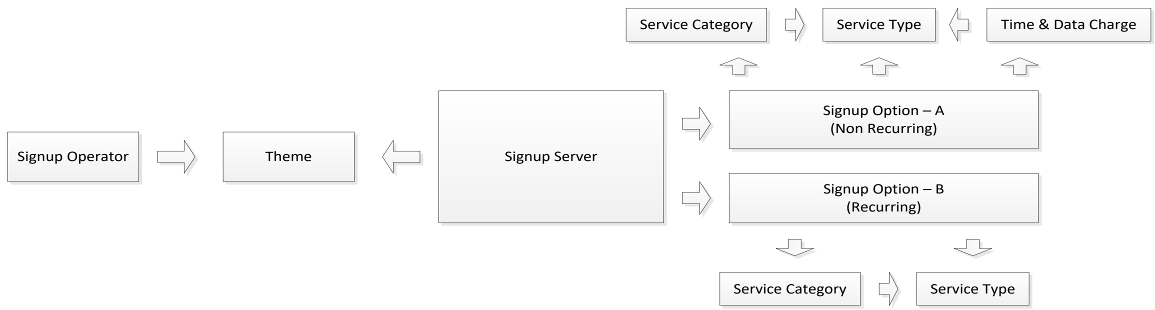
```
To insure correct company name and license key is entered use "cut & paste"
to enter license key and company name from license Email.
```

Signup Servers

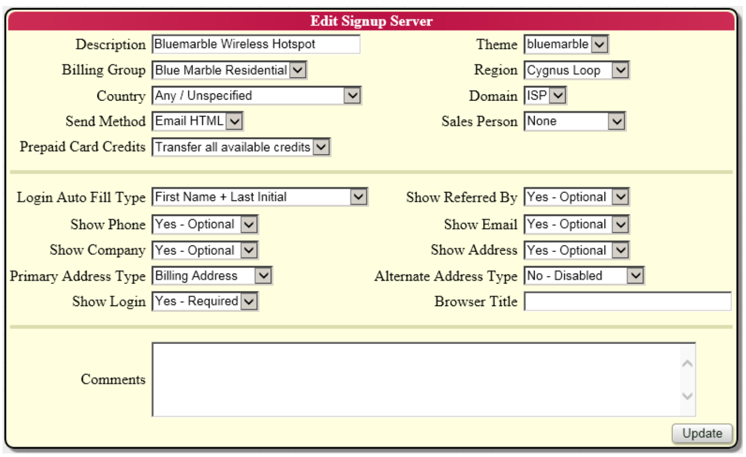
Emerald integrated signup server enables new customers to sign-up and fund new service automatically. Each signup server configured within this menu is able to provide unique sets of service options custom "themed" for each represented venue and organization.



When getting started with signup server configuration we recommend you begin by creating a list of service options you would like offered thru signup server. Make sure supporting service categories and service types have been defined from "Emerald Admin" / "Services" menu. For non-recurring service such as an Internet Hotspot time & data charges must also be defined to enable nonrecurring time and data purchases. Before proceeding with signup server configuration everything required to enable an operator to manually provision the same types of service options as those offered thru signup server should already be in place.



Next important prerequisite is signup operator and themes. Signup process begins with user "logging on" to Emerald as a signup operator. This is normally achieved by users clicking a provided "signup" hyperlink from company website or hotspot welcome page to begin signup process. Current theme of signup operator determines which signup server is presented to the user. Generally speaking for each signup server a theme and signup operator (assigned "CustomerSignup" operator group) will be required.



Field	Description
Description	Text describing purpose and venue or provider of this signup server
Theme	Theme associated with this signup server. Only one signup server can be associated with any one theme. When an operator with operator group of "CustomerSignup" logs on to Emerald theme chosen for operator's session must match signup server's theme configured in this field.
Billing Group	Billing Group new signups are to be assigned
Region	Sets MBR Region when creating account
Country	If set all users of this signup server are assumed to be located in specified country.
Domain	Sets service level Domain when creating account
Send Method	Sets MBR level Send Method when creating account
Sales Person	Sales person to credit the new signup (MBR and Service level sales person)
Prepaid Card Credits	When "Transfer all available credits" and a prepaid card is used to fund signup operation full prepaid credit amount remaining available to the card is transferred to new accounts balance even in cases where cost to open new account is significantly less than cards remaining available balance. This is the default and recommended setting. When "Transfer invoiced cost only" only amount necessary to initially open new account is transferred from prepaid card. This allows one card to be used to fund multiple separate signup operations. If there is insufficient balance remaining on card to fund initial signup

<table>
<tr><td></td><td>another card with sufficient balance must be provided.</td></tr>
<tr><td>Allowed Pay Methods</td><td>Configures acceptable methods of payment for purchase made during signup process. Allowed pay methods does not apply post-signup within customer account center or operator interfaces.

<table>
<tr><th>Pay Method</th><th>Description</th></tr>
<tr><td>Renewal</td><td>Normally unused for nonrecurring accounts.

For recurring service customer will remit payment for services manually normally by check, prepaid voucher or one-time credit card payment.</td></tr>
<tr><td>Credit Card</td><td>Initial payment by credit card.

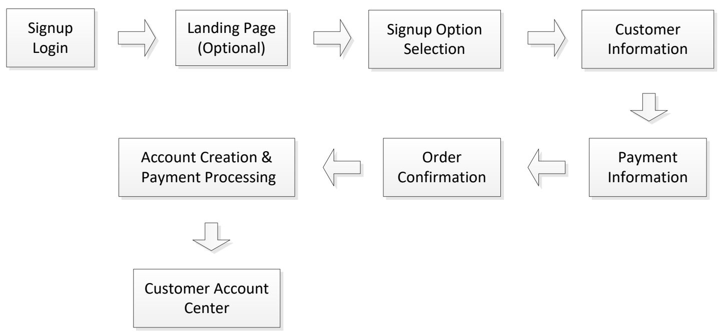
For recurring service subsequent invoices are paid automatically using credit card.</td></tr>
<tr><td>Pre-Paid Card</td><td>Initial payment by prepaid voucher.

For recurring service subsequent invoices are treated as "Renewal" requiring manual payment.</td></tr>
</table></td></tr>
<tr><td>Login Auto Fill Type</td><td>Sets the default value of the customer login field based on given information such as First and Last Name.</td></tr>
<tr><td>Show Referred By</td><td>When "Yes" the referred by field is displayed in the signup form</td></tr>
<tr><td>Show Phone</td><td>When "Yes" customer phone fields are displayed in the signup form</td></tr>
<tr><td>Show Email</td><td>When "Yes" the email field is displayed in the signup form</td></tr>
<tr><td>Show Company</td><td>When "Yes" the company field is displayed in the signup form</td></tr>
<tr><td>Show Address</td><td>When "Yes" customer address fields are displayed in the signup form</td></tr>
<tr><td>Primary Address Type</td><td>Address type to be used as primary billing address of the account</td></tr>
<tr><td>Alternate Address Type</td><td>An additional optional address type to allow for an extra address to be recorded during signup process. Commonly used to record service address when different from billing address.</td></tr>
<tr><td>Show Login</td><td>When "Yes" service login field is displayed in the signup form</td></tr>
<tr><td>Show Start Date</td><td>When "Yes" service starting date is displayed in the signup form to customize when service is to begin. Start date is only applicable to recurring service. Signup options with non-recurring cycle types are not affected by start date.</td></tr>
<tr><td>Browser Title</td><td>Sets the default title in the browsers title bar appearing on each signup server page. If no title is set the default browser title is "Emerald Management Suite"</td></tr>
<tr><td>Comments</td><td>For informational use only. Comments are not displayed within signup server.</td></tr>
</table>

When linking to signup server the signup operators login credentials are entered as part of the URL. For example:

<A HREF="https://demo.iea-software.com/login.ews?user=signup&password=signup">Click here to signup</A>

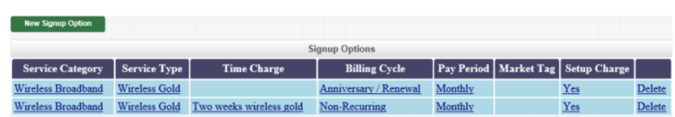
Signup Process

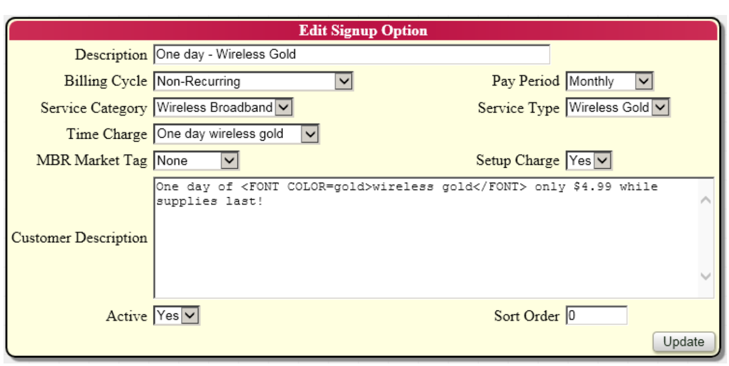


Step	Description
Signup Login	New customer logs into Emerald using the signup account or login credentials are provided automatically via URL link from an external site.
Landing Page	Optional initial page displayed prior to displaying a list of available service options to the user. Landing page is configured by customizing theme file "signup_intro.ews".
Signup Option	List of available signup options presented to the customer for selection.
Customer Information	Provides for collection of Customer contact information such as Name, Address, Login and Password. Customer information fields can be hidden from view or made required or optional when defining signup server to customize amount of detail required from customers.
Payment Information	Provides for collection of Customer payment related information such as selection of a pay method and any necessary pay method related data such as credit card or prepaid card account numbers.
Order Confirmation	This area provides an overall summary of selected package and customer entered data. Enables customer to review their signup for errors or changes before committing to sign up for new services.
Account Creation & Payment	After an order is confirmed by customer and customer input validated account is created and any initial invoices and payments are applied.
Customer Account Center	Once customer account is created the user is automatically logged into customer account center where they can then make further changes to their account or check status of invoices and payments. More information on customer account center is available from Emerald 6 customer account center documentation.

Signup Options

Once signup server is created signup options provide a selection of service plans to the user to choose from.

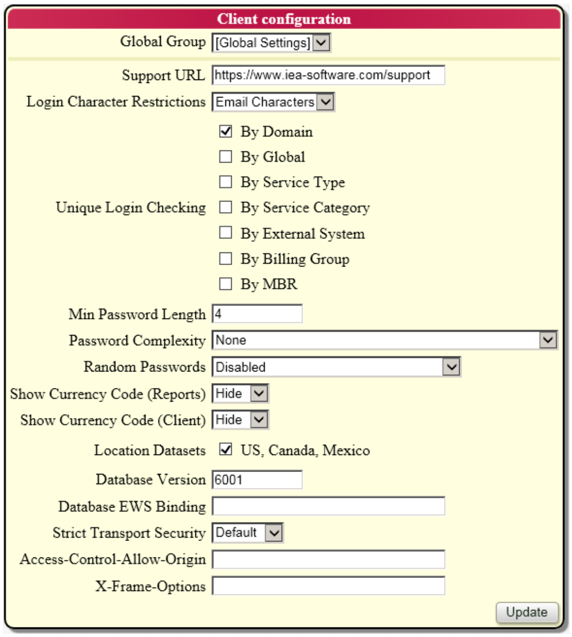




Field	Description
Description	Description of signup option displayed to the user within signup server
Billing Cycle	Billing cycle of an account created with this signup option
Pay Period	Sets default pay period of MBR and service for subscription based customers billed on a recurring basis. When a non-recurring billing cycle is chosen pay period field is ignored. Initial term of non-recurring accounts is defined by time charge selected below.
Service Category	Service category to be used when creating customers service. Only service categories allowed to be used as "root category" having compatible billing group with signup server are displayed.
Service Type	Service type within service category to be used when creating customers service. When non-recurring billing cycle is used only service types where one or more matching time charge was configured are displayed. If an expected service type of the service category above is not displayed please check "Emerald Admin" / "Accounting" / "Time & Data Charges" to confirm one or more time charge is available.
Time Charge	When non-recurring billing cycle is used the chosen time charge determines service cost and associated credit provided in terms of service expiry, session duration and data usage.
MBR Market Tag	Optional manual MBR tag to be activated when signup server is used to create an account using this signup option.
Setup Charge	Controls whether any applicable setup charge should be charged or waived. In order for a setup charge to be billed the chosen service type must be configured with one or more setup charges.
Customer Description	This field is used when presenting text of signup options to users. Description should include full outline of service including pricing, relevant access levels and restrictions. HTML tags may be used to customize presentation.
Active	When "Yes" the signup option is available to be selected for this signup server doing new account signup.
Sort Order	Controls sequence signup options are presented during signup process in ascending order.

Client Settings

When managing accounts from Emerald client this menu offers access to display and validation settings.



<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Global Group</td><td>When "Global Settings" is selected options set in this form apply globally to all billing groups not having a group specific configuration. Billing groups having a different configuration from the global group appear with "*" before their names.</td></tr>
<tr><td>Support URL</td><td>Help URL displayed in error forms throughout Emerald.</td></tr>
<tr><td>Unique Login Checking</td><td>Manages duplicate checking of service level login field. Each enabled option further constrains subset of related services to be checked for duplicate login.

For example if only "By Billing Group" is enabled then duplicate login checking is limited to members of the same billing group. If both "By Billing Group" and "By Service Type" is enabled duplicate checking is limited to members of the same group who also have the same service type.

If all unique login options are not checked then unique login checking is completely disabled.

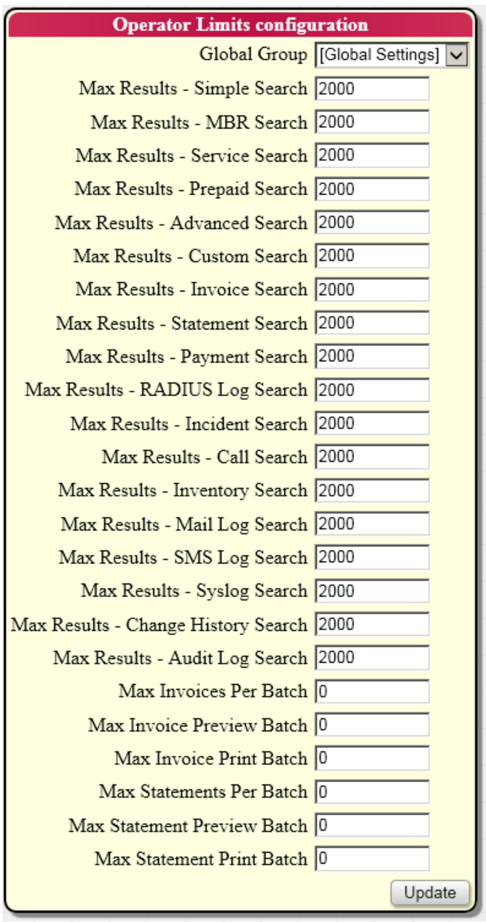
<table>
<tr><th>Unique Login</th><th>Description</th></tr>
<tr><td>By Domain</td><td>Login checking limited to services with matching service level domain.</td></tr>
<tr><td>By Global</td><td>Login checking across all services system wide.</td></tr>
<tr><td>By Service Type</td><td>Login checking limited to services with matching service type.</td></tr>
<tr><td>By Service Category</td><td>Login checking limited to services with matching service categories.</td></tr>
<tr><td>By External System</td><td>Login checking limited to services with one or more common external system assignments. If no external systems are assigned to the service then this option has the same effect as "By Service Type" limiting duplicate login checking to services of the same service type.</td></tr>
<tr><td>By Billing Group</td><td>Login checking limited to services with matching billing groups.</td></tr>
<tr><td>By MBR</td><td>Login checking limited only to services of the same MBR.</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>Exclude MBR</td><td>All current service logins under the same MBR are exempted from duplicate login checking. This enables multiple services within the same MBR to share the same logins where it would otherwise not be allowed. This setting is incompatible with "By MBR" above. If both By MBR and Exclude MBR are checked the outcome is the same as if "By MBR" is enabled and "Exclude MBR" disabled.</td></tr></table>
Login Character Restrictions	Determines acceptable characters when entering service login information. Chosen limitations apply only to service level Login field.
Password complexity	Mixed case, letter, number and symbol requirements for service level passwords. This setting and min password length are overridden by group rights security menu option if configured.
Min Password Length	Minimum allowed MBR Service password length
Random Passwords	Options for automatic password selection when adding new services to an MBR.
Show Currency Code (Reports)	When "Yes" organizations three-letter currency code is displayed throughout Emerald reports wherever currency values are shown.
Show Currency Code (Client)	When "Yes" organizations three-letter currency code is displayed throughout Emerald operator interface wherever currency values are shown.
Location Datasets	Specifies which location datasets should be updated or installed when an updated version of Emerald Suite is installed.
Database Version	Contains current internal database version number. If installed product version is higher than current internal database version Emerald database is automatically updated when Emerald web server starts upon first access to Emerald from a web client. Setting database version to a lower number such as "10" and then restarting Emerald will trigger database update. This can be useful to resynchronize Emerald database if stored procedures or configuration defined features have been damaged or when rolling back to a previous version of Emerald. If database version is set –1 no database updates will be executed against the Emerald database even when a new version of Emerald Suite is installed. This should never be done as mismatch between database version and Emerald software is very likely to lead to failure of the software to operate.
Database EWS Binding	Please do not make changes to this field unless directed by IEA support personnel.
Strict Transport Security	When 'Default' the strict transport security setting in security menu of Emerald configuration server controls whether HSTS is enabled. When Enabled the strict transport security setting within Emerald configuration server is ignored. For details about strict transport security please see the table in security menu documented above.
Access-Control-Allow-Origin	Overrides restrictive default Cross Origin Resource Sharing (CORS) policy to allow third party websites to programmatically access Emerald via client browser system wide for all ews requests. If specified value entered here (Normally * or https://mytrustedsite.example) is transmitted as header value within http response. If not specified Access-Control-Allow-Origin and Access-Control-Allow-Credentials headers are not transmitted in http response.

	This option should normally be left blank. Setting this header increases risk of targeted attacks on multifactor authenticated sessions.
X-Frame-Options	Overrides frame options response header with custom value. If no frame options are specified the header is transmitted with a default value of SAMEORIGIN. To prevent any X-Frame-Options header from being transmitted use special value "allow". This setting increases risk of targeted attack.

Operator Limits

Operator Limits determine maximum count of records returned by search operations globally and operator group basis. For all fields a value of 0 indicates no limit is enforced.

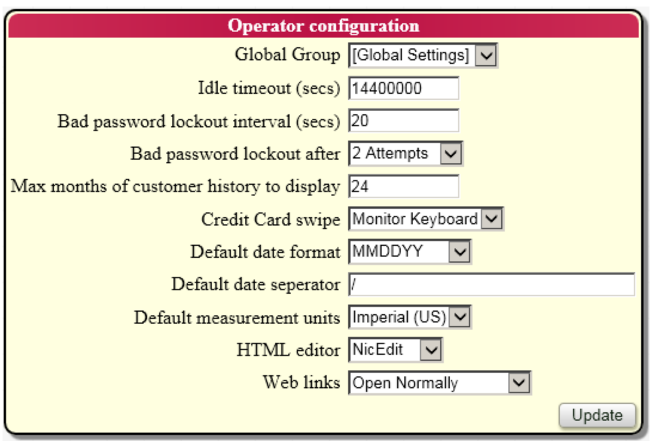


Field	Description
Global Group	When "Global Settings" is selected the options set in this form apply globally to all billing groups not having a group specific configuration. Billing groups having a different configuration from the global group appear with a "*" before their names.
Max Results ***	Maximum rows returned by account search operations
Max Invoices Per Batch	Total number of invoices allowed to be created for any single invoicing run. May be used to split up large invoice runs throughout time.

Max Invoice Preview Batch	During invoice previews from Emerald Client / Billing / Create Bills menu limits number of invoices that may be displayed for preview.
Max Invoice Print Batch	Invoices added to the print queue for postal delivery from Emerald Client / Billing / Send Bills menu are restricted in their per print batch count of invoices by this field. Feature is often used to make processing and printing more manageable with a large subscriber base.
Max Statements Per Batch	Total number of statements allowed to be created for any single invoicing run. May be used to split up large statement runs throughout time.
Max Statement Preview Batch	During statement previews from Emerald Client / Billing / Create Bills menu limits number of statements that may be displayed for preview.
Max Statement Print Batch	Statements added to print queue for postal delivery from Emerald Client / Billing / Send Bills menu are restricted in their per print batch count of statements by this field. The feature is often used to make processing and printing more manageable with a large subscriber base.

Operator Settings

System wide operator security and locale defaults are configured from this menu.

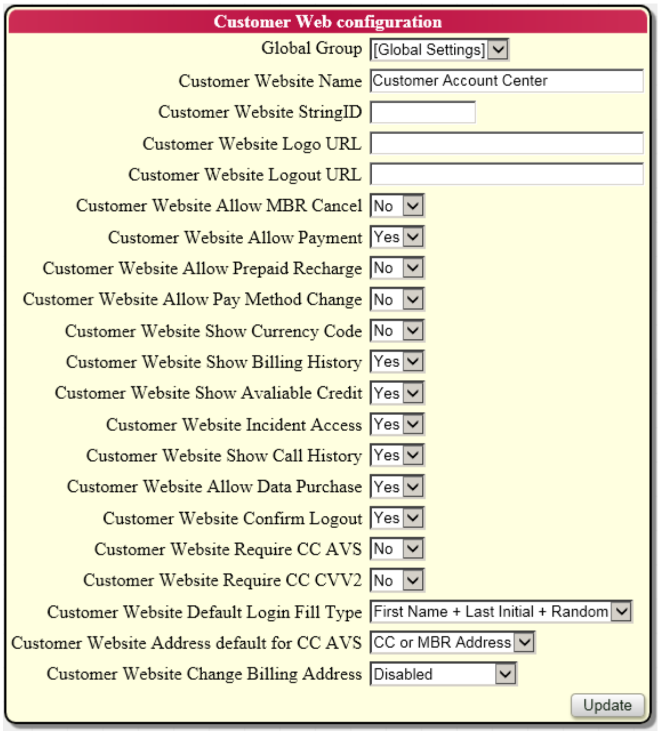


Field	Description
Idle timeout (secs)	Count of seconds between operator client web requests with no activity before timing out and forcing the user to logon again to access Emerald. Enter the value in number of seconds. This value must be greater than 300.
Bad password lockout interval (secs)	When an operator attempts more than "Bad password lockout after" times to authenticate within lockout interval operator is prevented from attempting to login until the lockout interval has passed. Feature is intended only to mitigate online dictionary attacks against weak operator passwords at some risk of being leveraged to prevent known operators from logging on to Emerald. Lockout applies to all usernames entered regardless of whether username is valid. This feature is not intended to be used as a long term/permanent account lockout. In the event multiple Emerald servers are used for

	high availability temporary lockouts are not shared across servers. All currently active lockouts are reset when the Emerald web server is restarted.
Bad password lockout after	Selected number of attempts occurring within lockout interval after which temporary lockout should be enabled per unique login name.
Max months of customer history to display	Controls maximum number of months of account history to show in the MBRs history display.
Max months of timeline changes to display	Number of months back of timeline changes relative to effective date displayed within MBR and service level timelines. A setting of 0 displays all active changes without regard for effective date.
Credit Card Swipe	When enabled operators browser listens for keyboard input from barcode scanners and credit card readers automatically bringing up appropriate account information within Emerald when a card swipe or barcode scan is detected. When disabled no keyboard monitoring is performed.
Default date format	System default date format to use when not defined via operator preference.
Default date separator	System default date separator to when not defined via operator preference.
Default measurement units	System default when presenting distances and weights in imperial or metric units.
Default time format	System default time of day format to use when not defined via operator preference.
Default account search status	When searching for accounts from Emerald Client / Accounts menu this option determines value of 'Status' field that will be used by default until changed by operator and after pressing 'clear' to reset a search form.
HTML editor	WYSIWYG editor used when sending HTML formatted bulk mail or configuring message body of HTML formatted notices. When set "None" the operator must manually manage any HTML tags to control formatting of HTML content.
Web links	When "Open Normally" operator facing web links within the operator dashboard and MBR address location links are rendered as standard hyperlinks. When "Open in New Window" web links are opened in a separate browser window or tab.

Customer Settings

Customer Account Center general options and access rules are configured both globally and per billing group basis via this menu.



Field	Description
Global Group	When "Global Settings" is selected the options set in this form apply globally to all billing groups not having a group specific configuration. Billing groups having a different configuration from the global group appear with a "*" before their names.
Customer Website Name	Title displayed at the top of customer account center before menu options. Default value is "Customer Account Center"
Customer Website StringID	Provides language support for the "Customer Website Name" field above.
Customer Website Logo URL	URL of a logo image to display in the Customer Account Center directly above the "Customer Website Name" title bar. Used for simple branding of the account center on a global and per billing group basis.
Customer Website Logout URL	After a customer manually logs out of the customer account center by selecting the "Log Off" menu option they can be directed to the URL specified here instead of the default Emerald Login screen if no value is entered in this field.
Customer Website Allow MBR Cancel	When "Yes" services with "Manager" remote access enabled are allowed to cancel their entire MBR via the customer account center interface. When "No" MBR level cancellation is disabled for accounts via the customer account center however cancellation on a per service basis may still be permitted depending on service type configuration within the accounts service category.
Customer Website Allow Payment	When "Yes" customers are allowed to make payments directly from the customer account center.
Customer Website Allow Prepaid Recharge	When "Yes" customers are allowed to use a new prepaid access card to recharge the account expiration, time left, data left and credit amount based on what is available on the new prepaid card.

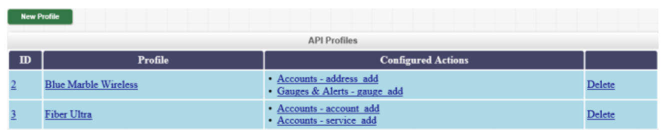
	For recharge to work the card must have "Direct Use" enabled and must have a direct use service type matching the end-users service type.
Customer Website Payment on Credit Balance	When "Yes" customers are not prohibited from making a manual credit card payment as a consequence of having a zero or credit balance. When "No" customers are prohibited from making manual credit card payments when they have a zero or credit balance. "No" is the default recommended setting to minimize possibility of unintentional overpayment.
Customer Website Payment on CC/EFT Auto	When "Yes" customers are not prohibited from making a manual credit card payment as a consequence of their account being configured for CC/EFT auto pay. When "No" customers are prohibited from making manual credit card payments when their account is on CC/EFT auto pay. "No" is the default recommended setting to minimize possibility of unintentional overpayment.
Customer Website Allow Pay Method Change	When "Yes" customers with "Manager" remote access enabled are allowed to change their current pay method to choose manual or automatic payment via credit card.
Customer Website Show Currency Code	When "Yes" the organizations three-letter currency code is displayed throughout the Emerald customer center wherever currency values are shown.
Customer Website Show Billing History	When "Yes" and "Manager" remote access is enabled a history of the MBRs invoices, statements and payments are visible from the Customer Account Centers "Billing Info" page.
Customer Website Show Available Credit	When "Yes" available credit amount based on MBR credit limit and current account balance is displayed in the account status area of the customer center. When "No" or MBR credit limit is 0 then credit limit information is not displayed.
Customer Website Incident Access	When "Yes" customers are able to add new incidents, add actions to existing incidents and view all incidents in their account with Customer Access enabled from the Assistance link in the customer account center. Note when upgrading from Emerald 4.5 customer access is disabled during the database upgrade for all pre-existing incidents.
Customer Website Show Call History	When "Yes" records of customers RADIUS call history are available from the "Usage History" menu within the account center. Accounts with "Manager" remote access enabled can view the account history of all services within the MBR while those without "Manager" remote access enabled can view only their accounts usage.
Customer Website Allow Data Purchase	When "Yes" accounts are able to make one-time service access purchases from the customer account center via the "Purchase Time" menu option. See "Admin" / "Accounting" / "One Time Charges" for additional information.
Customer Website Allow Promo Codes	When "Yes" customers are able to apply any valid applicable promo codes to their account from Manage Account / My Account Settings area of customer center.
Customer Website Confirm Logout	When "Yes" a JavaScript confirm dialogue is displayed when accounts in the customer account center choose the "Log Off" menu option. When "No" the customer is logged out and not

	shown the confirm dialogue.
Customer Website Require CC AVS	When "Yes" customer making credit card payments must submit Address information in order for the transaction to be accepted. Note the enforcement of an AVS match and availability of AVS matching is not controlled by this menu option. This field simply makes inputting of address information a requirement.
Customer Website Allow EFT	When "Yes" EFT is available for making one-time payments or setting bank account on file for EFT auto pay. Display of one time and auto pay options follows same rules as credit cards. When "No" EFT is not available to customer for making one time payments or setting bank account on file for EFT auto pay. This is the recommended default setting. In certain settings particularly hotspot environments where customers may only signup on a non-recurring basis for days of service allowing customer select EFT as a payment method may provide increased risk of fraud. Unlike credit card processing EFT transactions take days to process and no funds are blocked in real-time as with credit cards. Transactions are generally always approved up front by the transaction gateway even when customer has entered a completely invalid account or routing number.
Customer Website Child Service Management	When "Manager Access" and a customer logs on to the customer account center ability to manage child services of the service used to login requires service level "Remote Access" to be set "Manager". When "Manager or Service Access" and a user logs on to customer account center ability to manage child services of the service used to login requires service level "Remote Access" to be set "Service" or "Manager". If a service has only "Service" access the service used to access customer center itself cannot be managed. Only its immediate children are able to be managed.
Customer Website Require CC CVV2	When "Yes" customer making credit card payments must submit the CVV2 security code found on their credit cards. Due to usage rules the CVV2 code is cleared directly after the card transaction has completed. Automatic recurring credit card payments cannot transmit CVV2 information. It is against Visa and others operating rules to modify the Emerald transaction system to retain this data. When "No" entering of CVV2 data is optional.
Customer Website Default Login Fill Type	When an account adds a new service from the customer account centers "Manage Accts" menu the selected fill type is used to automatically set a default login name based on the fill type criteria such as First and Last Name.
Customer Website Address default for CC AVS	When entering credit card information within the customer center for one-time payment and when updating card on file for automatic payment this setting controls acceptable sources of default address information. When "CC or MBR Address" is used default card address will prefer credit card address on file. If no credit card is on file the MBR billing address is used instead. When "CC Address" only the credit card on file may be used to set default billing address.

	When "None" the credit card address defaults to blank requiring customers to manually enter address for AVS.
Customer Website Change Billing Address	When not "Disabled" customers may add or update an MBR level address of the selected address type. It is recommended an address type be designated exclusively for use by customers to change their billing address on file with a higher billing address priority than normal "billing" address type. This allows operator configured address on file to be retained rather than updated by customers to reduce any fraudulent use and allow old address to remain with the MBR and searchable.

API Profiles

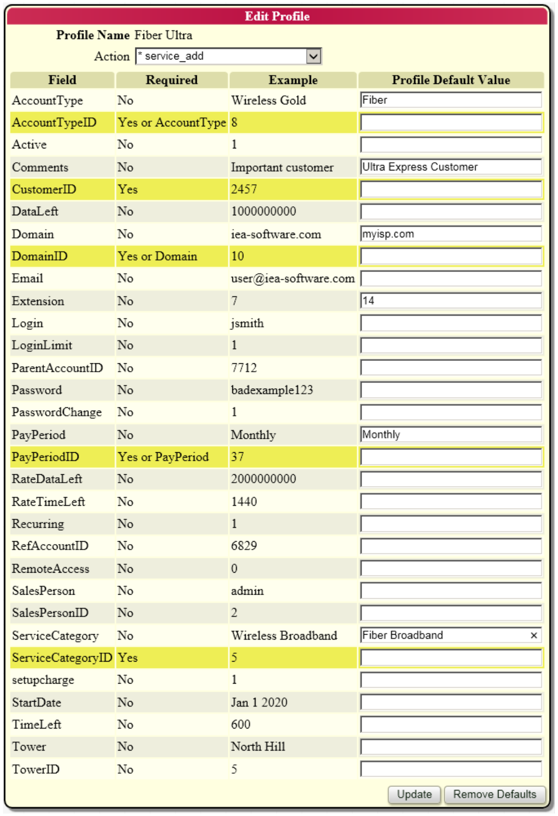
Profiles serve as a convenience for developers utilizing Emerald API to apply default settings while making API calls.



When a profile is configured profile specific default values are settable for any available API function. This enables developers to focus on fields unique for each situation while providing a convenient and abstract means of storing default configuration data.

In an example scenario wireless access accounts are provided from a third party partner where only the parameters Name, Address, Login and Password are provided.

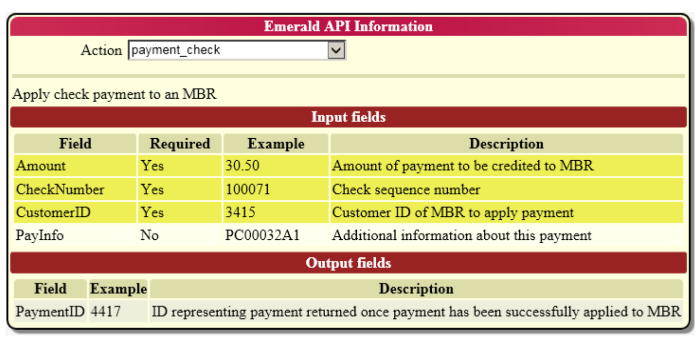
In this case a third party wireless profile is created to set defaults for all remaining necessary fields (billing group, billing cycle, region, sales person, referred by, default pay period, pay method, send method, service pay period, service category, service type, service domain, remote access and login limit) reducing information necessary to be supplied to create these wireless accounts.



Field	Description
Profile Name	Uniquely describes purpose of profile. This value is supplied in the "profile" input parameter to API calls to select profile for use.
Action	List of currently available API "actions" where default values may be configured. Actions beginning with an asterisk '*' are currently configured for use with this profile.
Profile Default Value	Action specific field to set default value. If left blank no default is applied. If there are questions about the use of specific actions and fields more information is available from API Info menu.
Remove Defaults	Removes all default settings for this profile associated with currently selected action.

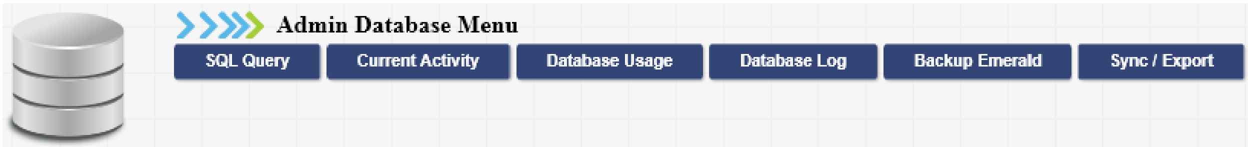
API Info

This menu item provides developers with details about all available Emerald API actions including overview of the action itself, input parameters and outputs. Actions related to functionality Emerald is currently not licensed are not displayed.

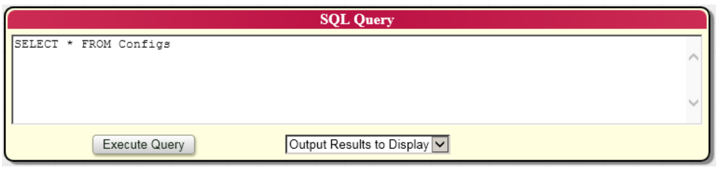


DATABASE

Database section of Emerald Administrator allows you to perform basic database functions including running queries and monitoring status of database server.



SQL Query



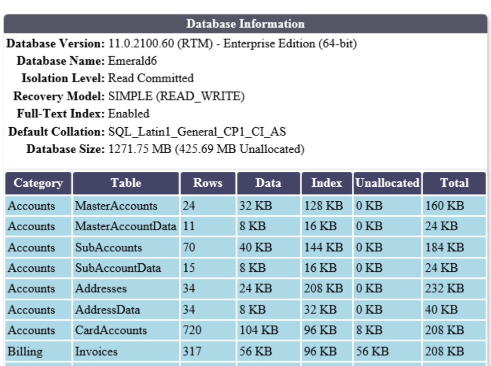
The query tool is primarily intended for use as a support tool. Global admin operators are able to execute SQL queries on Emerald database and output results (first result set only) to screen or download results in CSV, TSV, Excel, HTML and XML formats. It is recommended operators avoid using this query tool to make changes to any data or to execute anything which changes the database connections environment as connections are pooled and unexpected environment changes may interfere with operation of Emerald. If it should be necessary to make changes to Emerald data directly we recommend first backing up Emerald database and then using a query tool such as SQL Management studio where changes are able to be tested within a transaction and rolled back should it become necessary.

Current Activity

Current Activity shows each database process on your database server and related status information. Depending on conditions and database platform last or current SQL command that was or is executing on that connection is displayed. Processes may be killed manually from options column of current activity display.

When used with SQL Server processes are displayed with red background for processes blocked by or blocking other processes. This occurs normally and does not by itself indicate a problem or "deadlock" has occurred.

Database Usage



Database Information

Database Version: 11.0.2100.60 (RTM) - Enterprise Edition (64-bit)
Database Name: Emerald6
Isolation Level: Read Committed
Recovery Model: SIMPLE (READ_WRITE)
Full-Text Index: Enabled
Default Collation: SQL_Latin1_General_CP1_CI_AS
Database Size: 1271.75 MB (425.69 MB Unallocated)

Category	Table	Rows	Data	Index	Unallocated	Total
Accounts	MasterAccounts	24	32 KB	128 KB	0 KB	160 KB
Accounts	MasterAccountData	11	8 KB	16 KB	0 KB	24 KB
Accounts	SubAccounts	70	40 KB	144 KB	0 KB	184 KB
Accounts	SubAccountData	15	8 KB	16 KB	0 KB	24 KB
Accounts	Addresses	34	24 KB	208 KB	0 KB	232 KB
Accounts	AddressData	34	8 KB	32 KB	0 KB	40 KB
Accounts	CardAccounts	720	104 KB	96 KB	8 KB	208 KB
Billing	Invoices	317	56 KB	96 KB	56 KB	208 KB
Billing	InvoiceItems	2202	360 KB	144 KB	56 KB	560 KB

Database usage includes basic information about database server including version, edition, database name and overall size. Detailed information of data usage by table including number of rows and data consumed for row storage and index is also presented. Not all tables are displayed. Only those tables where data is stored where storage requirements are expected to vary significantly over time are included.

Performance Stats

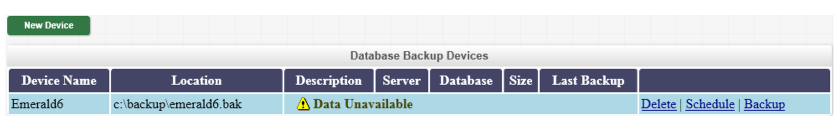
Searchable interface to the query store on SQL Server 2016 and later provide statistical details about the operations of database including duration, CPU, reads, writes, call counts, row counts and waits. For each query in search results following the detail link provide historical charting of monitored parameters over previous two weeks.

In search results rows appearing with light gold background have at least one call with duration of 5 or more seconds. Search matches any substring found in the query such as names of tables, fields and procedure names. To search the query store at an earlier point in time change the interval to the desired period over the last 7 day period.

Database Log

When using SQL Server the current database server log is displayed. Server log can sometimes be useful when troubleshooting database server related problems. The same log information is stored in the file ERRORLOG in the SQL Servers log folder.

Backup Emerald



When Emerald is used with Microsoft SQL server "Backup Emerald" allows Emerald database to be backed up to a file accessible to the database server. Functionality is limited when compared with database backup and maintenance wizard included with SQL Management Studio and is intended for use only with those customers using Emerald without SQL agent to perform automatic backups. We recommend using SQL Management Studio when available to configure backup and maintenance schedules for Emerald database.

Database backups created from this menu are standard SQL Server backup files. They can be restored normally using SQL Management studio. Backup and restore operations are managed entirely by database and are not specific to Emerald.

To create a scheduled backup add a new backup device pointing to the full path and filename on disk where the backup file will be stored. File storage is relative to the computer and account the database server is hosted. Next select 'Schedule' from the listing of backup devices to schedule recurring backup. To create a one-time select 'Backup'.

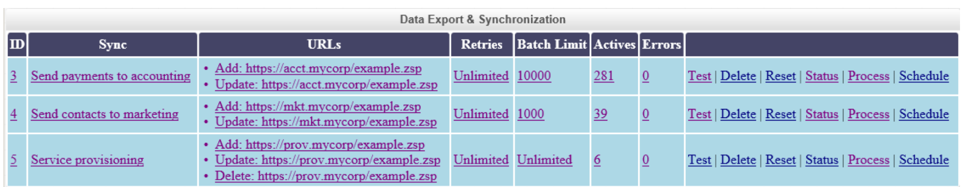
Sync / Export

Quick sync enables data within Emerald to be transmitted to an external system or custom ews templates and continually updated as new data is created, changed or withdrawn. This system works by defining a SQL query whose result set determines data transmitted and synchronized with the external system.

Each row of query result set is transmitted as a separate standard web post request to the external system. Each field of the result set is transmitted as a form variable with a label corresponding to column label of SQL query result set.

Once the external system successfully acknowledges receipt only new, changed or withdrawn data is subsequently transmitted as a result of future changes to query result set. Required state is managed automatically providing simplified synchronization for a wide range of data from Emerald to the external system.

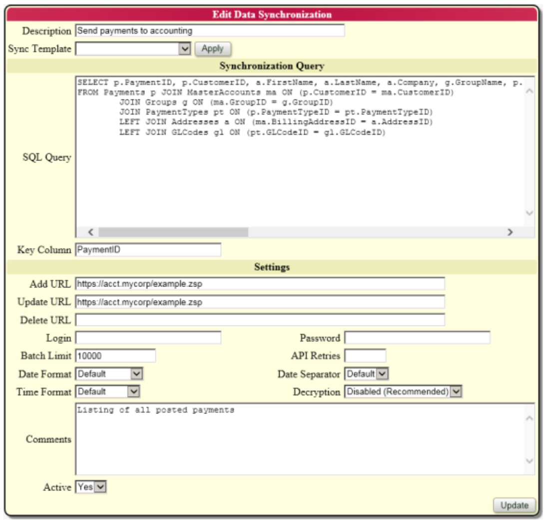
Syncs are scheduled to run periodically keeping external system updated with any changes to the dataset.


Data Export & Synchronization

ID	Sync	URLs	Retries	Batch Limit	Actives	Errors	
3	Send payments to accounting	• Add: https://acct.mycorp/example.zsp • Update: https://acct.mycorp/example.zsp	Unlimited	10000	281	0	Test | Delete | Reset | Status | Process | Schedule
4	Send contacts to marketing	• Add: https://mkt.mycorp/example.zsp • Update: https://mkt.mycorp/example.zsp	Unlimited	1000	39	0	Test | Delete | Reset | Status | Process | Schedule
5	Service provisioning	• Add: https://prov.mycorp/example.zsp • Update: https://prov.mycorp/example.zsp • Delete: https://prov.mycorp/example.zsp	Unlimited	Unlimited	6	0	Test | Delete | Reset | Status | Process | Schedule

Option	Description
Test	Performs full processing of sync query except no data is exported to the external system and no state changes are applied to the database. Intended to assist in troubleshooting sync related configuration issues.
Reset	Irreversibly removes all accumulated synchronization state collected as changes are accepted by external system. After a reset all rows of the sync query are presumed to be new to the external system and exported accordingly. Reset is typically used when replacing an external system or replacing its internal database.
State only	Generates synchronization state necessary to deem all current sync query data fully synchronized without transmitting any changes to external system URLs. This is typically used in cases where the external system only wants to be notified of new changes going forward rather than starting from the beginning and transmitting all data that happens to match the sync query.
Status	Search for and examine recorded synchronization state and view details of any synchronization errors reported by external system or sync while posting to external system.
Process	Manually start sync. When there are many records to export it may take some time for processing to complete and status to be displayed. Normally sync is run periodically from the scheduler and

	realtime status information is available from scheduler current status display.
Schedule	Schedule is only displayed when a scheduled task has not yet been created to process the sync. Clicking schedule link creates a scheduled task to periodically sync data. If schedule link is not displayed then sync has already been scheduled. Scheduled tasks are managed from configure schedules menu of the scheduler.



Field	Description
Description	Unique description for this sync. Field is displayed in the listing of syncs.
Sync Template	When creating a new sync selecting from a template which most closely matches your needs offers a sample SQL query as a starting point for customization. When a sync template is applied existing fields (SQL Query, Key Column and Decryption) are replaced with template specific settings.
SQL Query	SQL Query defines dataset to be exported and synchronized to the external system. Query must return a single result set with column labels corresponding to the labels of form variables to be transmitted in a web POST request to the external system. Query must contain a key column typically the primary key of the dataset that is unique across all rows of the dataset. It is recommended results be unordered. Order results are processed in is not preserved and may be transmitted in any order. When exporting data add operations are processed first followed by updates and finally deletions. If a sync query is expected to return many millions of rows system resources required for sync may be reduced using any of the following strategies. • Configure scheduled task of the sync to run less often. • Configure a batch limit to restrict number of post requests to external system within any single run of sync process. This reduces sync memory usage and limits flooding of external system with sync requests. • Create additional syncs and filters in SQL query to retrieve only the latest additions or latest changes by matching fields such as creation and last modify date rather than all data of interest. This shifts filtering responsibilities from application to database reducing database resource consumption.

Key Column	Column name from result set of SQL Query indicating key column used to uniquely identify a row of data. Key column will typically reflect primary key of underlying table. No row of the result set can have a key column exceeding 64 bytes in length.
Add URL	HTTP(S) URL of external system for receiving new records having not previously been synchronized. If omitted external system is not notified of new records added to result set. URL may alternately be filename of a custom ews template located within Emerald\web folder.
Update URL	HTTP(S) URL of external system used for receiving changes to one or more fields associated with records that have been previously successfully added and then changed. If omitted external system is not notified of updates to existing records of result set. URL may alternately be filename of a custom ews template located within Emerald\web folder.
Delete URL	HTTP(S) URL of external system used for receiving notice of withdrawal of record from result set after having been previously successfully added. Only the key column of the removed record is posted. Delete means the record is no longer contained within the result set of SQL Query and does not necessarily indicate the underlying record was removed from the database. If a previously deleted record is subsequently reintroduced in a future result set it is treated as a new record. If omitted external system is not notified of records withdrawn from result set. URL may alternately be filename of a custom ews template located within Emerald\web folder.
Login	Used to authenticate sync to the external system. The contents of the login field are posted to the external system using a form variable labeled "SyncLogin". If both Login and Password are provided credentials are also passed using standard HTTP authentication header.
Password	Used to authenticate sync to the external system. The contents of the password field are posted to the external system using a form variable labeled "SyncPassword". If both Login and Password are provided credentials are also passed using standard HTTP authentication header.
Batch Limit	Maximum number of calls to Add URL and Update URL allowed within a single run of sync process. Batch limit does not apply to Delete URL. Setting a batch limit can reduce local memory use while processing a large result sets. Limits also allow large datasets to initially be absorbed incrementally over time with each run of the sync process. If batch limit is left blank or less than 1 no batch limit is imposed.
API Retries	Limits count of API failure responses from external system before no further attempts are made for a given row of result set. Only API failure response where the external system returns a nonzero retcode XML or JSON element is counted as an API failure. All other failure causes such as DNS lookup failure, TCP/TLS connection failures or non-API responses without retcode element are not counted as an API failure and do not contribute to retry limit. If a batch limit is set API retries can be used to limit the possibility of long term repeated API failures preventing or limiting the processing of other records which have not failed because the batch limit was consumed by failed attempts. If API retries is left blank or less than 0 no retry limit is imposed. Retry limit of 0 disables retry. API retries can be raised or removed at any time to resume processing of any failed rows having reached their API retry limit.
Date Format	Manages formatting of any date fields in the query result set transmitted to the external system. By default the configured system defaults are used.
Date Separator	Manages formatting of any date fields in the query result set transmitted to the external system. By default the configured system defaults are used.

Time Format	Manages formatting of any time fields in the query result set transmitted to the external system. By default the configured system defaults are used.
Decryption	When enabled any encrypted data fields contained within the result set are first decrypted prior to export. HTTPS URLs should be used for communication with external systems to provide for authentication of external system and confidentiality.
Comments	Additional information
Active	When inactive sync cannot be executed manually or via scheduled task. Disabling External System Exports under Upgrade & Testing also effectively inactivates all syncs.

Upon receipt of post request the external system referenced by Add URL, Update URL or Delete URL returns either XML or JSON elements "retcode" in body of response indicating success or failure to process the request. Upon failure "message" element indicates plaintext failure cause.

XML success example:

```
<response><retcode>0</retcode></response>
```

JSON success example:

```
{"retcode":0}
```

XML failure example:

```
<response><retcode>-1</retcode><message>Insufficient resources to process request</message></response>
```

JSON failure example:

```
{"retcode":-1,"message":"Insufficient resources to process request"}
```

When a local ews template file is referenced rather than an external URL and the template completes without aborting it is considered success. Template processing aborted via $abort command within template or an error handler is treated as a failure.

Example

In this example a new sync is created with SQL query "**SELECT AddressID, FirstName, LastName, Company FROM Addresses**", Key Column "**AddressID**", Login "**my sync login**" and Password "**my sync password**".

SQL Query returns the following result set:

AddressID	FirstName	LastName	Company
1	Tom	Anderson	Metal Corp
2	Steve	Neklaf	Daron
3	Kate	Yvool	Ellingson Mineral

Given above example sync shall transmit equivalent of executing the following HTML in a web browser to post to external system for add or change operations. Separate requests are transmitted for each row of the queries result set after a new row is added to the result set or an existing row has changed.

```
<FORM METHOD=POST ACTION="Add or Update URL">

<INPUT TYPE=HIDDEN NAME="AddressID" VALUE="1">

<INPUT TYPE=HIDDEN NAME="FirstName" VALUE="Tom">

<INPUT TYPE=HIDDEN NAME="LastName" VALUE="Anderson">

<INPUT TYPE=HIDDEN NAME="Company" VALUE="Metal Corp">

<INPUT TYPE=HIDDEN NAME="SyncLogin" VALUE="my sync login">

<INPUT TYPE=HIDDEN NAME="SyncPassword" VALUE="my sync password">

<INPUT TYPE=SUBMIT VALUE="Test">
```

For delete operations only the key column is transmitted to indicate record has been withdrawn from result set.

```
<FORM METHOD=POST ACTION="Delete URL">

<INPUT TYPE=HIDDEN NAME="AddressID" VALUE="1">

<INPUT TYPE=HIDDEN NAME="SyncLogin" VALUE="my sync login">

<INPUT TYPE=HIDDEN NAME="SyncPassword" VALUE="my sync password">

<INPUT TYPE=SUBMIT VALUE="Test">
```

When a local ews template file is referenced rather than an external URL ews template is executed once per row with Variables table containing columns from the sync query.

```
$update.Addresses

Comments=Account updated

FirstName=$Variables.FirstName

LastName=$Variables.LastName

Company=$Variables.Company

AddressID=$Variables.AddressID

error_include=update_error.ews

$update
```

APPENDICES

Appendix A - Supported Third Party External Systems

The Emerald Management Suite works with many different third-party products. The open nature of the Emerald database and the technical specifications of the suite allow third party applications to easily interact with Emerald. Please see IEA Software product site for Emerald 6 for an up-to-date list.

https://www.iea-software.com/emerald6

Appendix B - Generic Web Service Account Synchronization

Generic web service synchronization enables Emerald to notify a custom "web service" API of changes to status of accounts managed by Emerald. Leveraging this system initial provisioning and state synchronization of services can be maintained between Emerald and a user defined provisioning system.

External System Configuration

Create a new external system from the Emerald Admin / Services / External systems menu. Choose 'Generic Web Service' from the System Type menu. Configure the URL of your user defined web service that will be consuming provisioning requests. The login and password fields are mapped to the APILogin and APIPassword post request parameter fields in the table below.

General API Instructions

For each item being processed the API sends a POST request containing form variables to a user defined URL for processing and expects an XML formatted response in return.

POST Request Parameters (From Emerald to External system)

Field Name	Type	Description
APILogin	String	Login used to authenticate Emerald to the external API. (Configured via External systems)
APIPassword	String	Password used to authenticate Emerald to external API (Configured via External systems)
APIRef	String	Reference field to identify the Emerald external system to external API (Configured via External systems)
CustomerID	Integer	Customer ID (MBR level ID) of the account
AccountID	Integer	Account ID (Service level ID) of the account
Domain	String	Configured mail domain of the service
chDomain	Integer	When 1 field is new or changed. When 0 then field has not changed.

<table>
<tr><td></td><td></td><td>(See above)</td></tr>
<tr><td>Login</td><td>String</td><td>Service login field. Login field must not be blank in order to be successfully provisioned.</td></tr>
<tr><td>chLogin</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>Password</td><td>String</td><td>Service password field. Password field must contain at least two characters to be successfully provisioned.</td></tr>
<tr><td>chPassword</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>FirstName</td><td>String</td><td>First name of the service</td></tr>
<tr><td>ChFirstName</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>LastName</td><td>String</td><td>Last name of the service</td></tr>
<tr><td>chLastName</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>ServiceType</td><td>String</td><td>Reflects service type label of current service type</td></tr>
<tr><td>chServiceType</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>ExternalRef</td><td>String</td><td>Service type specific reference field to map service type to external system concept of ‘type of service’. (Configured via the Service Types - External Systems menu)</td></tr>
<tr><td>chExternalRef</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>Alias</td><td>String</td><td>When a service email alias is configured reflects a single alias from the list of aliases. Note: If more than one alias is configured only a single alias is presented.</td></tr>
<tr><td>chAlias</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>Forward</td><td>String</td><td>When a service email forward is configured reflects a single mail forward from the list of forwards. Note: If more than one forward is configured only a single forward is presented.</td></tr>
<tr><td>chForward</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
<tr><td>Action</td><td>String</td><td>Generic record change status
<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td>add</td><td>Record has not previously been exported to the external system.</td></tr>
<tr><td>update</td><td>One or more fields of the existing record has changed.</td></tr>
<tr><td>delete</td><td>The service and or MBR has been inactivated and the underlying account should be removed</td></tr>
</table></td></tr>
<tr><td>Active</td><td>Integer</td><td>When 1 the account is active and in good standing. When 0 and the action variable above is not "delete" the account has been temporarily suspended due to expiration/nonpayment. The user should not be allowed to access to normal services. The service should not be marked for permanent deletion. Background activities such as collection of Email messages should continue.

When the action variable is "delete" the service should be considered to be permanently inactive and any steps necessary for removal should be taken. No further provisioning messages will be issued for this account.</td></tr>
<tr><td>chActive</td><td>Integer</td><td>When 1 field is new or changed. When 0 then field has not changed. (See above)</td></tr>
</table>

Post Response Parameters (From external system to Emerald)

Response must be XML formatted.

Field Name	Type	Description
Retcode	Integer	Indicates status of the provisioning request. When 0 then the request was successful. Any other value means the provisioning request has failed. Any failed requests are retried the next time external system synchronization is run.
Message	String	Text field indicating the status of the provisioning request. When retcode is 0 the contents of the message field is ignored. When retcode is non-zero (request failed) Message is a descriptive text indicating the failure cause. Message is displayed in the show service menu of the Operators services interface if the retcode field indicates a failure.

Response example for successfully processed request:

```
<retcode>0</retcode><message>looks good</message>
```

Response example for failed request:

```
<retcode>-1</retcode><message>not enough resources to complete request</message>
```

Appendix C - Emerald API

API offers programmatic access to Emerald client for external management of accounts and related data facilitating automation and integration with third party systems.

Interface protocol and formatting

Emerald API is layered over HTTP. Input variables are transmitted as GET or POST (recommended) variables to Emerald server. No other HTTP request verbs are supported.

All API responses are XML or JSON formatted within body of HTTP response containing an API layer status indication transmitted as XML or JSON formatted RETCODE field. Value of 0 indicates success, any other value indicates failure. Upon failure MESSAGE field contains additional information relating to failure reason. XML formatting is used by default unless format=json parameter is included. See Calling API below for more details.

When processing API requests it is recommended that all non-2xx class HTTP responses and all 2xx class responses without properly formatted API layer status be treated as non-API layer failures.

Please note API Authentication failure does not provide an XML formatted response if non-TLS level authentication fails.

Since HTTP protocol is not inherently transactional it is recommended a transaction token first be obtained prior to making API calls affecting data to allow for detection of uncommon failures that could result in a loss of synchronization between API callers and Emerald.

Authentication & Security

Authentication can be accomplished using any of the following methods:

1. Transmit API operator login credentials with each API call using login_user and login_password input parameters.
2. Obtain a session cookie by passing API login credentials (login_user and login_password parameters) to /api_login.ews. Once COOKIE is obtained it may be transmitted in Cookie header of subsequent API calls until session is no longer valid.
3. TLS layer mutual authentication (curl -k --tlsuser … --tlspassword …)

Client certificates may optionally be used in conjunction with any of the above authentication methods.

API operators must be assigned an operator group dedicated to API access. This API cannot be accessed from any operator group with access to Emerald UI including by global administrators. To create new API operator group add "API" object group to an empty operator group. Next add additional "API ***" object groups as appropriate to grant needed access. Please refer to Emerald Admin / Security / "Object Group Info" for more details regarding access provided by each group. All account related API calls respect billing group level access settings.

It is not recommended this API be consumed directly by web browsers. All API calls are intentionally not CSRF protected.

Transaction tokens

Tokens optionally provide protection against uncommon failure conditions such as sudden network or system interruptions during an HTTP transaction that may result in loss of synchronization between API caller and Emerald data.

To use tokens:

1. Obtain a single-use token by calling /api_token.ews. There are no input parameters except what is necessary for authentication (login_user, login_password) token is returned in TOKEN field.
2. Make an API call (/api.ews) passing input parameter of token equal to TOKEN value in step 1 above.

Only upon successful completion of step 2 will the token be consumed. If the caller tries to repeat any API call previously completed successfully using the same token the API call is canceled with RETCODE of -12.

Retention period of unused and claimed tokens is configured from Emerald Admin / Reports & Logs / Log Trimming / Trim days for API tokens. Retention is 1/2 year by default.

Resource	Description
/api_token.ews	Obtains transaction token. No input parameters (except authentication) Output example: <RESPONSE><TOKEN>43</TOKEN><RETCODE>0</RETCODE></RESPONSE>
/api_token_status.ews	Checks the current status of a token. Input parameter "token" Output example: <RESPONSE><CREATEDATE>01/18/17 0:23:39</CREATEDATE> <COMMITDATE></COMMITDATE> <LOCKED>0</LOCKED> <RETCODE>0</RETCODE></RESPONSE>

API Profiles

When a profile is configured profile specific default values are settable for any available API action. This enables developers to focus on fields unique for each situation while providing a convenient and abstract means of storing default configuration data. Please see API Profiles for more information.

Calling API

API is located at /api.ews relative to Emerald server.

To use this API call /api.ews with following POST method input variables:

Field	Required	Description
login_user	Yes or TLS Auth	Username of operator account for API access. The operator account must be assigned to an operator group dedicated for API access. Existing operator groups for access to Emerald UI including global administrator accounts cannot be used in conjunction with API.
login_password	Yes or TLS Auth	Password of operator account for API access.
action	Yes	Represents API action to be executed. For listing and descriptions of all available actions see Emerald Admin / Web Interface / API Info.
profile	No	API Profile name containing default values for specified action. For more information see Emerald Admin / Web Interface / API Profiles
token	No	Optional transaction token previously obtained by calling /api_token.ews
format	No	When set output format can be changed from XML to one of the following formats. **Format** — **Description** csv — Any API output containing tabular data will be comma separated values (CSV) formatted and include a column header. All other API responses are XML formatted. tsv — Any API output containing tabular data will be tab separated values (TSV) formatted and include a column header. All other API responses are XML formatted. excel — Any API output containing tabular data will be MS Excel

<table>
<tr><td></td><td></td><td><table>
<tr><td></td><td>formatted XML. All other API responses are XML formatted.</td></tr>
<tr><td>json</td><td>Any API output containing tabular data will be formatted as a JSON array with one object per row. All other API responses are in the form of a JSON formatted object.</td></tr>
</table></td></tr>
<tr><td>** See API Info</td><td>**See API Info</td><td>Action specific input parameters per API Info documentation.

In case of optional fields where no value is intended to be transmitted field should not be transmitted with an empty value. This is because generally when a field is not transmitted it is interpreted as not indicating a preference allowing any database level default which may exist to be applied. Sending field with no value generally indicates the field's value is intended to be empty.</td></tr>
</table>

HTTP response body contains XML formatted variables:

<table>
<tr><th>Field</th><th>Presence</th><th>Description</th></tr>
<tr><td>RETCODE</td><td>Always</td><td>Provides feedback on whether the API call was successful.

<table>
<tr><th>Code</th><th>Description</th></tr>
<tr><td>0</td><td>Action was successful</td></tr>
<tr><td>-1</td><td>General failure, see MESSAGE</td></tr>
<tr><td>-10</td><td>Action specific input requirement check has failed</td></tr>
<tr><td>-11</td><td>Access control or security related error</td></tr>
<tr><td>-12</td><td>Provided transaction token invalid or previously claimed</td></tr>
<tr><td>-13</td><td>Referenced profile does not exist or not configured to support action.</td></tr>
<tr><td>-14</td><td>Data add/modify/delete errors</td></tr>
<tr><td>-15</td><td>Referenced action is unknown or inactivated</td></tr>
</table></td></tr>
<tr><td>MESSAGE</td><td>Upon failure</td><td>Contains additional information about any failures when RETCODE is nonzero.</td></tr>
<tr><td>** See API Info</td><td>** See API Info</td><td>Action specific outputs per API Info documentation.</td></tr>
</table>

API Examples

Update credit card on file.

https://localhost/api.ews?action=cc_modify&customerid=1&cardnumber=4444333322221111&expirationdate=Jan+1+2020&CardHolder=John+Smith&login_user=api&login_password=dontuseget

<RESPONSE><RETCODE>0</RETCODE></RESPONSE>

Get an API token:

https://localhost/api_token.ews?login_user=api&login_password=dontuseget

<RESPONSE><TOKEN>44</TOKEN><RETCODE>0</RETCODE></RESPONSE>

Error response - record gauge data using a non-existent profile and token returned from above example:

https://localhost/api.ews?login_user=api&login_password=dontuseget&action=gauge_add&data=2.3121&datetime=jan+17+2017+11:33:22&profile=test&token=44

<RESPONSE><MESSAGE>No profile data is available for action 'gauge_add' using profile 'test'</MESSAGE>

<RETCODE>-13</RETCODE></RESPONSE>

JSON formatted response - record gauge data using a non-existent profile and token returned from above example:

https://localhost/api.ews?login_user=api&login_password=dontuseget&action=gauge_add&data=2.3121&datetime=jan+17+2017+11:33:22&profile=test&token=44&format=json

{ "retcode":"-13","message":"No profile data is available for action 'gauge_add' using profile 'test'"}

Appendix D - Report Post-Processing

Once a report has been rendered post-processing allows custom external programs to be called to modify or archive the rendered report.

Post-processing configuration

To enable post-processing of reports set following registry/ini keys manually.

Configuration registry or file locations:

Operating System	Location
Windows 32-bit view	HKEY_LOCAL_MACHINE\SOFTWARE\IEA\EmerWeb
Windows 64-bit view	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IEA\EmerWeb
Linux	/usr/local/emerald/emerweb.ini

Configuration keys:

Key	Description
ReportPostCMD	Full pathname of the external post-processing program to be called by Emerald immediately after rendering report.
ReportPostMask	A bitmask of output destinations. See output destinations below and add up the ID columns of the destinations you would like to be processed to arrive at value. For example to enable notification and emailreport value of ReportPostMask is 6 (2 Notification + 4 emailreport)

<table>
<tr><td></td><td><table>
<tr><th>ID</th><th>Output Destination</th></tr>
<tr><td>1</td><td>Output to display / browser</td></tr>
<tr><td>2</td><td>All reports rendered from notification system (includes batch invoice and statement emailing)</td></tr>
<tr><td>4</td><td>Reports rendered from "emailreport". (One-off Invoices and Statements sent manually from MBR invoices and statements menu)</td></tr>
</table></td></tr>
<tr><td>ReportConvertCMD</td><td>While not used for post processing this configuration may be used to customize external HTML to PDF conversion processing. If specified any configured format conversion processor is replaced with entered command.

Input contains only a single parameter containing full pathname of the HTML rendered report.

Post processing command is expected to read this file and replace its contents with PDF version returning exit code 0 when completed. If failure occurs post processing command is expected to exit with a non-zero value.</td></tr>
</table>

External post-processing program interface

Immediately after a report is rendered external post-processing program referenced by the key ReportPostCMD is called by Emerald with following ordered command line parameters. The program must block until all post-processing tasks have been completed.

<table>
<tr><th>Parameter #</th><th>Description</th></tr>
<tr><td>1</td><td>Full pathname of the report file used to render report. (e.g. "c:\program files\emerald\web\reports\statement.ews")</td></tr>
<tr><td>2</td><td>Integer representing output format of the rendered report based on the table below.

<table>
<tr><th>ID</th><th>Format</th><th>Supported By</th></tr>
<tr><td>1</td><td>HTML</td><td>Emerald & Crystal</td></tr>
<tr><td>2</td><td>PDF</td><td>Crystal</td></tr>
<tr><td>4</td><td>RTF</td><td>Crystal</td></tr>
<tr><td>8</td><td>Word</td><td>Crystal</td></tr>
<tr><td>16</td><td>Text</td><td>Crystal</td></tr>
<tr><td>32</td><td>XML</td><td>N/A</td></tr>
<tr><td>64</td><td>CSV</td><td>N/A</td></tr>
</table></td></tr>
<tr><td>3</td><td>Output destination for report describing means by which fully rendered report is to be presented.

<table>
<tr><th>ID</th><th>Output Destination</th></tr>
<tr><td>1</td><td>Output to display / browser</td></tr>
<tr><td>2</td><td>All reports rendered from notification system (includes batch invoice and statement emailing)</td></tr>
<tr><td>4</td><td>Reports rendered from "emailreport". (One-off Invoices and Statements sent manually from MBR invoices and statements menu)</td></tr>
</table></td></tr>
<tr><td>4</td><td>Full pathname of a temporary file containing rendered report.

If post-processing program modifies contents of this temporary file the modified contents are presented to the output destination.</td></tr>
</table>

	If the temporary file is moved or deleted the original rendered report is presented to the output destination. Once the report is transmitted to output destination this temporary file if still present is automatically removed from the file system.

Upon completion the post-processing program exits with code 0 on success. Any other exit code is interpreted as post-processing failure resulting in subsequent failure to output report.

Please note Emerald may concurrently execute any number of instances of the post-processing program simultaneously to handle multiple simultaneous reporting requests.

Appendix E - Detailed Account Synchronization

Detailed account web service synchronization enables Emerald to notify a custom external "web service" of changes to status of accounts managed by Emerald. Leveraging this system initial provisioning and synchronization of subsequent changes to MBR and service level data can be maintained between Emerald and a user defined provisioning system.

External System Configuration

Create a new external system from the Emerald Admin / Services / External systems menu. Choose 'Detailed Account Sync' from System Type selection. Configure URL of your user defined web service consuming provisioning requests from Emerald. Login, password and API Ref fields are transmitted as APILogin, APIPassword and APIRef POST Request Parameters below.

General API Instructions

For each item requiring synchronization Emerald sends a POST request containing form variables to the user defined URL for processing and expects an XML formatted response in return.

POST Request Parameters (From Emerald to External system)

Field Name	Description
APILogin	Login used to authenticate Emerald to the external API. (Configured via External systems)
APIPassword	Password used to authenticate Emerald to external API (Configured via External systems)
APIRef	Reference field to identify the Emerald external system to external API (Configured via External systems)
ESRef	Reflects value of external reference field configured where external system is assigned to service type in service type external system menu.
MBRExternalRef	MBR level external reference field

CustomerID	Customer ID (MBR level ID) of the account
AccountID	Account ID (Service level ID) of the account
Domain	Configured mail domain of the service
Login	Service login field
Password	Plaintext service password field
AccountType	Reflects service type label of the service
action	Data synchronization status **Action** – **Description** add – Record has not previously exported to the external system or was previously exported and subsequently successfully deleted due to inactivation of MBR or Service. update – One or more fields of the existing record have changed. delete – Service and or MBR has been inactivated or deleted and the underlying account should be removed
Status	Current service status **Status** – **Description** active – MBR and service are active and in good standing expired – Service has expired generally due to non-payment canceled – MBR and or service have been scheduled for temporary or permanent cancellation and cancel date has passed. inactive – MBR and or service have been inactivated deleted – MBR or service have been deleted
Recurring	When 1 the service is billed automatically on a recurring basis. When 0 the service is non-recurring and invoiced manually for continuing usage on an as-needed basis.
CancelReason	If the account is canceled or scheduled for cancellation in the future this field displays cancel reason. If no cancellation is scheduled this field is empty.
CancelDate	If the account is canceled or scheduled for cancellation in the future this field displays cancellation date. If no cancellation is scheduled the field is empty.
Region	MBR Region
PayMethod	MBR Pay Method **Pay Method** – **Description** Renewal – Customer pays for service manually using any available method Credit Card – Customer pays for recurring service automatically using credit card Bank Transfer – Customer pays for recurring service automatically using EFT
GroupName	MBR Billing Group
SendMethod	MBR delivery method for invoices and or statements
BillingCycle	MBR billing cycle
PIN	MBR account PIN for telephone customer verification
PayPeriod	For recurring service pay period reflects the term customer is invoiced.
Extension	Service permanent extension in days. This does not include MBR level temporary extension
SalesPerson	Sales person assigned to service
RemoteAccess	Service level access to customer account center self-management portal **Access** – **Description** Manager – Customer has full MBR level access to customer account center Service – Customer has limited service only access to customer account center

	None	Customer is unable to login to customer account center
LoginLimit	Service level concurrent login limit. If left blank no limit is configured for this account.	
Tower	Name of tower linked to this service	
BillFirstName	First Name	
BillLastName	Last Name	
BillCompany	Company	
BillAddress1	Address 1	
BillAddress2	Address 2	
BillCity	City	
BillState	State	
BillState2	State abbreviation	
BillZip	Postal Code	
BillCountry	Country	
BillCountry2	Country 2-letter abbreviation	
BillPhoneHome	Home Phone	
BillPhoneWork	Work Phone	
BillPhoneMobile	Mobile Phone	
BillEmail	Email	
BillLat	Address physical location Latitude	
BillLong	Address physical location Longitude	
ServiceFirstName	First Name	
ServiceLastName	Last Name	
ServiceCompany	Company	
ServiceAddress1	Address 1	
ServiceAddress2	Address 2	
ServiceCity	City	
ServiceState	State	
ServiceState2	State abbreviation	
ServiceZip	Postal Code	
ServiceCountry	Country	
ServiceCountry2	Country 2-letter abbreviation	
ServicePhoneHome	Home Phone	
ServicePhoneWork	Work Phone	
ServicePhoneMobile	Mobile Phone	
ServiceEmail	Email	
ServiceLat	Address physical location Latitude	
ServiceLong	Address physical location Longitude	
ContactFirstName	First Name	
ContactLastName	Last Name	
ContactCompany	Company	
ContactAddress1	Address 1	
ContactAddress2	Address 2	
ContactCity	City	
ContactState	State	
ContactState2	State abbreviation	
ContactZip	Postal Code	
ContactCountry	Country	
ContactCountry2	Country 2-letter abbreviation	
ContactPhoneHome	Home Phone	
ContactPhoneWork	Work Phone	

ContactPhoneMobile	Mobile Phone
ContactEmail	Email
ContactLat	Address physical location Latitude
ContactLong	Address physical location Longitude

Post Response Parameters (From external system to Emerald)

Response must be XML formatted.

Field Name	Type	Description
Retcode	Integer	Indicates status of the provisioning request. When 0 then the request was successful. Any other value means the provisioning request has failed. Any failed requests are retried the next time external system synchronization is run.
Message	String	Message is a descriptive text indicating the failure cause when retcode is non-zero. (request failed) Message is displayed in the show service menu of the Operators services interface if the retcode field indicates a failure.

Response example for successfully processed request:

<retcode>0</retcode><message>looks good</message>

Response example for failed request:

<retcode>-1</retcode><message>not enough resources to complete request</message>

Appendix F – Scaling and Redundancy

Recommendations for system scalability and availability are provided in the sections below.

Row Versioning

It's recommend operators experiencing delays due to locking or managing 50k or more active MBRs enable row versioning (RCSI) within their Emerald database. This feature is enabled by running the following query where 'Emerald6' is the name of your Emerald database.

ALTER DATABASE Emerald6 SET READ_COMMITTED_SNAPSHOT ON WITH ROLLBACK IMMEDIATE

The query can take a few minutes to complete and impacts system operation while running. Once enabled database read operations are no longer blocked by write operations reducing lock contention and improving scalability. As Emerald is designed to always assume optimistic concurrency no further changes are necessary.

Compression

Disk storage requirements can be significantly reduced by enabling database compression. This has the benefit of increasing volume of data server is able to cache in available memory while reducing I/O and storage requirements. Compression slightly increases CPU consumption and works by efficiently organizing database server's internal data structures for a select subset of tables. It is recommended all customers using SQL Server Express edition enable this feature to help ensure database size remains below 10 GB limit. To enable compression run the following query on your Emerald database. On large databases compression or decompression can take several minutes to hours to complete and should be performed during a maintenance window.

CompressDB

To remove compression:

DecompressDB

Database Memory Settings

While typically best way to maximize system performance is provisioning as much memory as possible the database server defaults are sometimes too aggressive. We advise manually configuring a maximum allowed upper memory limit a couple of gigabytes lower than installed ram within Memory tab of database server properties in SQL Server Management Studio (SSMS) to account for needs of operating system and other software that may be running on the same server in order to avoid excessive paging.

Emerald Concurrent Request Limits

Emerald allocates a fixed number of concurrent web requests and database connections at startup. By default 10 requests can be processed concurrently and up to 32 concurrent database connections are available for use at any given time. These settings are managed from the Emerald configuration server under Security and Database Settings.

Where there are many concurrent users or when accessing Emerald over wireless, international or satellite links with high latency it may be necessary to significantly increase concurrent request limit to avoid delays accessing Emerald. If there are multiple listen IPs configured each IP is allocated its own separate pool of concurrent requests. For example if concurrent request count is 100 and there are two listener IPs defined in the Emerald configuration server a total of 200 concurrent requests are allocated in total between both listeners.

Care should be taken when deciding to increase database connections to avoid diminishing returns where more concurrent database access reduces overall throughput. Database connection limits apply per datasource. If there are for example two datasources available and the concurrent database connection limit is 32 then a total of 64 database connections are possible provided both datasources are concurrently available for use.

Redundancy

SQL Server database mirroring and availability groups provide seamless automatic database failover in the event of failure of primary database server. Emerald supports multiple primary and secondary read only datasources for data redundancy.

Emerald application redundancy is implemented by installing two or more Emerald servers and connecting each to the Emerald database servers. All servers should be of same Emerald version. For redundant access to Emerald UI either round robin DNS or load balancers can be used.

If an Emerald server or service fails operator sessions are seamlessly resumed on remaining server(s) without loss of operator session state or data. Emerald background services including RADIUS, scheduler, SMS poller and session manager automatically assume the roles of failed services. Backup server licenses are included with Emerald enterprise or as add-on feature license of Emerald professional.

Appendix G - SMPP Technical Data

The following is intended to be a technical reference of the IEA Software SMPP implementation to aid in any interop or acceptance testing required by an SMS provider before the system can be used on the provider's network.

Question	Answer
Intended use	2-way messaging
SMPP Versions	3.4
SMPP PDU Transports	IPv4 – TCP, TCP-TLS, IPv6 - TCP, TCP-TLS
Bind Modes supported	Receiver, Transceiver
Outbind support	No
Concurrent binding & redundancy	Single TCP session to single SMSC is supported at any point in time. Backup server configuration is provided to allow failover should the primary become unavailable.
Connection policy	ESME attempts to maintain long-term connections to SMSC reconnecting only when necessary. Disconnect is not based on failure response to submit message requests or inactivity.
Enquire Link	Enquire Link requests are sent at 60 second intervals. Any valid incoming message from the SMSC resets both the Enquire Link timer and expectation of Enquire Link response. If no response is received in 30 seconds a network or app failure is assumed and the session is terminated.
Loss of protocol synchronization	Any validation failure while decoding PDUs is interpreted as a network failure. The connection is terminated without sending unbind request and a new connection is established.
Unbind messaging	Prior to disconnecting a TCP session the ESME sends an unbind request and waits for an unbind response up to 15 seconds before terminating the network connection unless a network problem is suspected and was the initial reason for disconnect. ESME honors receipt of SMSC initiated unbind request.
Bind failure back-off	All bind failures include a 5-minute back-off period before retry. Operators have the option of manually forcing an earlier retry after making SMPP configuration changes by clicking the “Apply” button after updating poller settings.

<table>
<tr><td>Response to credit/balance status messages</td><td>On receipt of no balance or credit errors the ESME unbinds from the SMSC and waits 5-minutes before attempting a new bind.</td></tr>
<tr><td>Response to throttle indication</td><td>On receipt of throttle indication the SMSC pauses for 15 seconds before sending any outgoing PDUs.</td></tr>
<tr><td>Outgoing rate limit</td><td>Outgoing rate limit configuration is supported. Rate limits are calculated based on a 10 second window.</td></tr>
<tr><td>Sequence numbers</td><td>Sequence numbers during an SMPP session are monotonically increasing and not reused.

On reconnect due to network problem or configuration change the sequence number is not reset. Between connections any queued delivery responses can be received and processed.

Sequence numbers are not kept in persistent storage and therefore reset to 1 when the server is restarted or rebooted.</td></tr>
<tr><td>User configurable SMPP fields.</td><td>System ID, Password, Source Address (submit) and Address Range.</td></tr>
<tr><td>Supported data encoding for Delivery</td><td>Character encodings supported for incoming SMS messages

<table>
<tr><th>Code</th><th>Description</th></tr>
<tr><td>0</td><td>Assumes GSM 7-bit alphabet</td></tr>
<tr><td>1</td><td>ANSI x3.4</td></tr>
<tr><td>3</td><td>ISO-8859-1</td></tr>
<tr><td>5</td><td>JIS-0208</td></tr>
<tr><td>6</td><td>ISO-8859-5</td></tr>
<tr><td>7</td><td>ISO-8859-8</td></tr>
<tr><td>8</td><td>UCS2</td></tr>
<tr><td>13</td><td>JIS-0212</td></tr>
</table></td></tr>
<tr><td>Supported data encoding for Submit</td><td>Character encodings supported for outgoing SMS messages
<table>
<tr><th>Code</th><th>Description</th></tr>
<tr><td>3</td><td>ISO-8859-1</td></tr>
<tr><td>8</td><td>UCS2</td></tr>
</table></td></tr>
<tr><td>Submit NPI/TON</td><td>
<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>SRC TON</td><td>0</td><td>Source number type: Unknown</td></tr>
<tr><td>SRC NPI</td><td>1</td><td>Source numbering plan: E.164</td></tr>
<tr><td>DST TON</td><td>1 (configurable)</td><td>Destination number type: International</td></tr>
<tr><td>DST NPI</td><td>1 (configurable)</td><td>Destination numbering plan: E.164</td></tr>
</table></td></tr>
<tr><td>Submit Transaction Mode</td><td>Assumes store and forward. No delivery receipt requested.</td></tr>
<tr><td>Submit retry</td><td>No message is ever retried more than 3 times. The following status codes are considered temporary – all others are permanent failures and never retried.

<table>
<tr><th>Failure Code</th><th>Description</th></tr>
<tr><td>0x00000410</td><td>SERVICETYPE_NA</td></tr>
<tr><td>0x00000014</td><td>RMSGQFUL</td></tr>
<tr><td>0x00000045</td><td>RSUBMITFAIL</td></tr>
<tr><td>0x00000058</td><td>RTHROTTLED</td></tr>
<tr><td>0x00000064</td><td>RX_T_APPN</td></tr>
</table>
Delivery response timeout is 400 seconds.</td></tr>
</table>

<table>
<tr><td>Submit large messages</td><td>Supported</td></tr>
<tr><td>Deliver large messages</td><td>Supported</td></tr>
<tr><td>GNACK</td><td>Supported and understood as a response to any request or as an unsolicited indication.</td></tr>
<tr><td>Response to unknown or unsupported commands</td><td>GNACK /w invalid command id status code</td></tr>
<tr><td>Supported command codes</td><td>Following SMPP command codes are supported

<table>
<tr><th>Code</th><th>Description</th></tr>
<tr><td>0x80000000</td><td>GENERIC_NAK</td></tr>
<tr><td>0x00000001
0x80000001</td><td>BIND_RECEIVER</td></tr>
<tr><td>0x00000009
0x80000009</td><td>BIND_TRANSCEIVER</td></tr>
<tr><td>0x00000004
0x80000004</td><td>SUBMIT_SM</td></tr>
<tr><td>0x00000005
0x80000005</td><td>DELIVER_SM</td></tr>
<tr><td>0x00000006
0x80000006</td><td>UNBIND</td></tr>
<tr><td>0x00000015
0x80000015</td><td>ENQUIRE_LINK</td></tr>
</table></td></tr>
<tr><td>Optional TLVs</td><td>Message payload</td></tr>
<tr><td>Maximum allowed incoming PDU length</td><td>512,000 bytes. Any single PDUs with a larger byte count are interpreted as loss of protocol synchronization.</td></tr>
<tr><td>TCP packet fragmentation</td><td>ESME attempts to emit non-fragmented PDUs and accepts fragmented PDUs.</td></tr>
</table>