EmerAuth

External Authentication DLL
Version 4.5.2

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 copies of 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. All images, photographs, animations, audio, video and text incorporated into the Software is owned by IEA Software, Inc., unless otherwise noted by Trademark.

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. Suite 201, West 416 Riverside Spokane, Washington 99201.

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 the 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. at Suite 326, West 422 Riverside Spokane, Washington 99201 U.S.A. (509) 444-2455.

Table Of Contents

1. Introduction

The Emerald Authentication DLL (EmerAuth) is an interface to the Emerald database which allows external systems (ES) to interact with the Emerald database without having to know the database schema or access the database directly. This decreases the challenge of vendors trying to keep up with the database structure or program an ODBC interface into their products. Tight integration alleviates users from having to manage multiple user databases and offers greater scaleability and control for all products.

When the ES starts up, it typically will initialize the DLL. At that point, the DLL will make a connection to the SQL Server and verify licensing and database consistency. After the DLL is successfully opened, the ES can call the available routines to verify and manipulate user data.

The DLL uses multiple connections to the SQL Server and can handle multiple requests simultaneously. It is multi-thread safe and designed for high performance. If the external system is broken into modules (for example a mail server might have several modules), each module can safely have their own instance of the DLL without interference to the other one. The DLL is intelligent enough to cache user information and re-connect broken or lost connections to the SQL Server.

EmerAuth is available either with a full Emerald license or a RadiusNT Enterprise license. It will not work with a standard RadiusNT license, and requires the license to be stored in the database rather than the in the registry.

IEA Software works directly with vendors to insure sufficient functionality is available. If you have additional questions about routines of the EmerAuth, please send mail to support@iea-software.com.

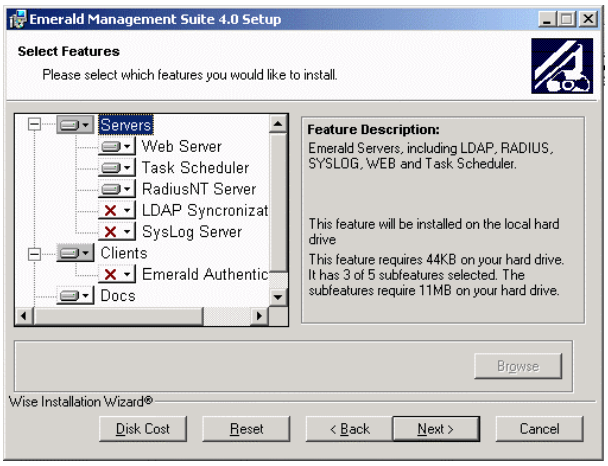
Supported Applications

EmerAuth includes five sets of APIs. The primary API is the generic user API, which is much more flexible and feature rich than the others. The other APIs are designed for specific software packages. Below is a list of vendors and software packages supported.

Application	Type	Vendor	Website
NTMail	Mail Server	Internet Shopper	www.ntmail.co.uk
IMail	Mail Server	Ipswitch	www.ipswitch.com
Serv-U	FTP Server	Cat-Soft	www.cat-soft.com
DNews	News Server	NetWin	www.netwinsite.com

2. Installation

You can install EmerAuth as part of the Emerald distribution by selecting the EmerAuth component during installation, as the EmerAuth component is not installed with the typical selection. To install EmerAuth Select the Custom option as your Installation Type. EmerAuth is located under the Client Option and is called Emerald Authentication DLL. Select the X next to Emerald Authentication DLL and select “will be installed on local hard drive.” Then select Next and EmerAuth will be installed with the distribution.



Alternately, if you have Emerald already installed, you can copy the eaadmin.exe and EmerAuth.dll files to your Emerald directory. Once copied there, start EmerAuth in configuration mode (see the configuration section) and select the install button (win32 only).

3. Configuration

Configuring EmerAuth is accomplished via the EmerAuth Configuration server.

Starting the EmerAuth Administrator

To start the EmerAuth Configuration server in initial configuration mode follow these steps:

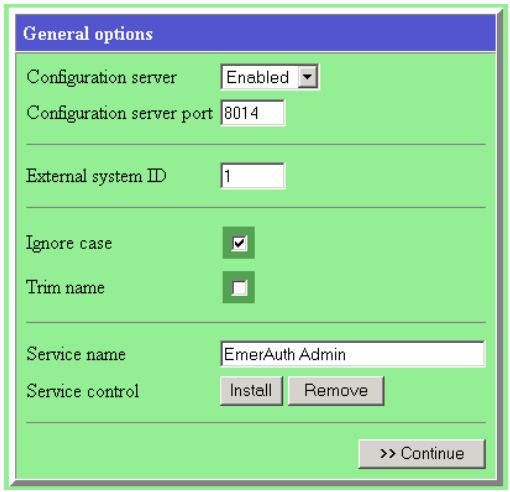
1. From your Start Menu, Program Files, Emerald, Server, select EmerAuth Admin Debug Mode.
2. From your Start Menu, Program Files, Emerald menu, select EmerAuth Web Config. When you are prompted for a password this is the admin password you set up in Emerald.

   Alternately (if you are manually installing EmerAuth):

   1. Open a command prompt and change to the directory where you installed EmerAuth. Within that directory, execute the command "Eaadmn –debug".
   2. Open a web browser and go to the URL: http://127.0.0.1:8014

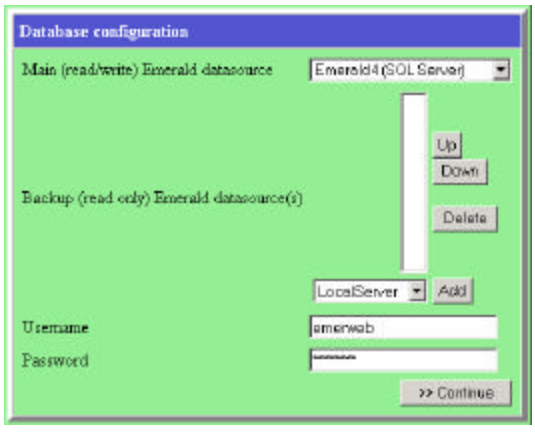
Configuring EmerAuth

1. Select the General options menu option. After changing the settings, click Continue.



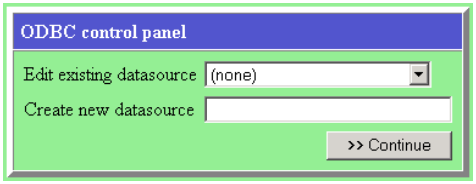
   - ?? Enable the Configuration Server and select a port. The default port is 8014.
   - ?? Enter the External System ID for the External System. This should have been setup in the Emerald Admin before you configure EmerAuth. Please see the below section on Mail Configuration for more details on setting up an External System ID.
   - ?? By default, RadiusNT/X is case sensitive when authenticating a username and password. If this option is enabled, RadiusNT/X will perform case in-sensitive comparisons for authentication.
   - ?? When enabled, the Trim Name option will cause RadiusNT/X to trim the domain prefix or suffix from a username.
   - ?? Set the service name if you are going to install or remove the service. You can select the Install and Remove options to install and remove the service.

2. Select the Database Configuration menu option. After changing the settings, click continue. **Please note, these settings are commonly shared between all Emerald servers. Therefore, if you already have Emerald or other Emerald server installed and configured on this machine, these settings should already be set. Changing these settings will affect all other applications as well.**



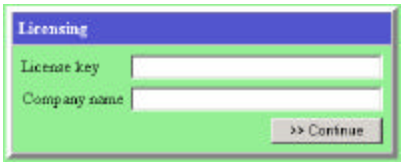
?? The Main Emerald datasource is the datasource that Emerald is using and the datasource that EmerAuth will use. This is the ODBC DSN that you will use to connect to the Emerald database. If you do not have a DSN defined, you can select (new) to create a new DSN.
?? The Backup Emerald datasource is any datasource to be used if the primary datasource in unavailable.
?? The username and password to connect to the database as.

3. The ODBC Control Panel can be used to create a new datasource or edit and existing datasource.



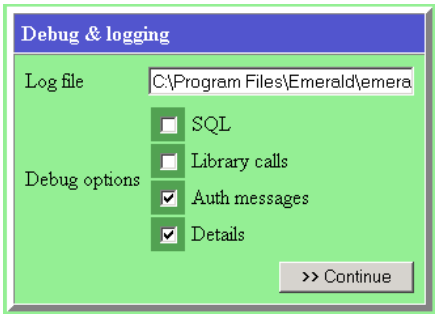
?? Select a data source item. This is the ODBC DSN that you will use to connect to the Emerald database. If you do not have a DSN defined, you can type the name of the new datasource in the Create New datasource field and then click continue. You will then be guided through creating a new datasource.

4. Select the Licensing menu option and enter your license information. After changing the settings, click Continue.



Note: A special key is required to run EmerAuth. Please email sales@iea-software.com if you have any questions regarding your key.

5. If you want to define debugging or logging, select the Debug and logging menu option. After changing the settings, click Continue.



?? Type the full path of where you want the log file.
?? Select the Debug options that you want to see when running in debug and what information you want written to the log file.

6. Once you have configured the server, it is very important that you choose the "Save Changes" 

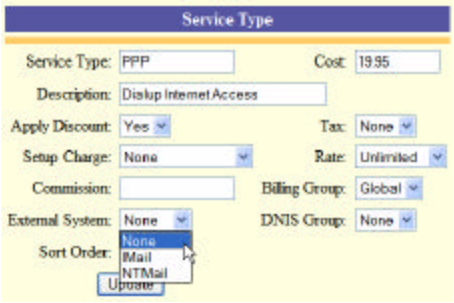
option from the top. Until you select this link, the options and changes you made will not be permanently stored. Also selecting the save changes links signals the server to reload the configuration options and start running under the new options.

Configuring External Systems

For each installation of EmerAuth that will be attached to a mail server, you should configure an External System in the Emerald Admin. In the General section, select the Domains option, and select New Domain. The mail domain field must match the domain configuration of the mail server. Domain is the field used in the pick list, and Description is just a long description for the domain. If you want the domain to be limited to a specific group, you can select that group. Sort Order is the order (from 0 as the first to 255 as the highest) to display the domain entries in.

In the System Section, select the External Systems option, and select New External System. The Name and Description fields are used to describe the External System. For External Option, select either External for NTMail or IMail for IMail. All other options should be left blank, as they do not apply to EmerAuth. Click the update button to save the External System. On the External Systems list, the ESID for each External System that you create is listed in the first column. You will need that number when configuring the ESID the EmerAuth Administrator.

Lastly, you must associate Service Types to the External System. If you have multiple mail servers this is how you tell Emerald which Services will be provisioned to each Mail server. In the Accounting Section, select the Service Types option. If you have existing Service Types that will have a mail account associated to them, select that service type. Otherwise, create a new service type.



For the Service Type, select the applicable External System and click the update button.

4. NTMail

Once you have the emerauth.dll file, you need to modify your NTMail registry settings to tell NTMail to use it. Below is a brief explanation of this process, but you should consult the NTMail Reference Manual to complete details.

Configuration

To configure NTMail to use the emerauth.dll authentication DLL, you need to add the following registry value:

```
HKEY_LOCAL_MACHINE\Software\InternetShopper\Mail\Parameters\UserDLLLocation
```

as type REG_SZ. You should copy the emerauth.dll file to your NTMail base directory and have the contents of the above key be "emerauth.dll".

Here is the information from the NTMail Reference Manual about this value:

> This defines the location and name of a security DLL. NTMail will use the specified DLL to validate unknown users. NTMail will search (in the order given) the following directories for the security DLL
>
> 1. BASEDIR\<UserDLLLocation>
> 2. %WINNT%\SYSTEM32\<UserDLLLocation>
> 3. <UserDLLLocation>

Additionally, there is a registry setting specific to the NTMail API that you need to set:

```
HKEY_LOCAL_MACHINE\Software\IEA\EmerAuth\ESID
```

This is the External System ID the user's service must belong to in order for the user to be considered a NTMail user. You can find out this number in the Emerald Administrator when you configure the External System. See below for more details.

How it works

When NTMail is re-started after the above change is made, it will verify the emerauth.dll file, by calling an init routine. This triggers the DLL to connect to the ODBC Datasource specified. You MUST have this configured before running NTMail or the external authentication will always fail. The ODBC DSN should point to an existing Emerald installation.

When a user logs in, NTMail asks the DLL to authenticate the user. The DLL will do a lookup in the Sub-Accounts table for one of:

1. a login matching the username, and the domain the MBR belongs to matching the domain of the authenticating user.

2. a shell matching the username, and the domain the MBR belongs to matching the domain of the authenticating user.

3. an email address matching the username and the domain of the authenticating user.

If any of the above match, NTMail will then ask the DLL for some additional user information, and based on whether its a POP3/IMAP4 or incoming message (no password validation is done on incoming messages), return the appropriate user info.

NTMail will search its own user database FIRST. If the user does not exist in the NTMail user database, then it will query the DLL. Therefore if you have a username in both, the NTMail will always take precedence over the Emerald user. Therefore, you can setup special users or features in NTMail if the option is not available in Emerald (like forwards, etc).

To restrict which users will be NTMail users, you can define an External System in Emerald 2.2 or higher of type NTMail. Then you can specify Service Types to belong to that External System (both of these are done in the Emerald Administrator). This is ideal if you have multiple mail servers or want to have multiple NTMail systems, since you can create multiple NTMail external systems and group your service types to different External Systems.

Known Problems

The default mailbox NTMail recommends is always returned. A future version will allow you to specify whether you want the user's mailbox to be in their Emerald home directory or not.

5. IMail

Although IMail allows you to add and edit users via the IMail admin and user manager, EmerAuth only allows the IMail Admin to read user information from the Emerald database. All functions that create/modify/delete user information will always return an error, as you should use Emerald for use management, not the IMail Admin user management portions. The only exception to this is setting the web preferences flag.

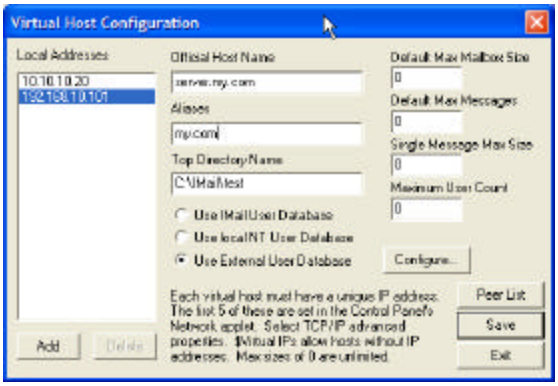
EmerAuth 4.5.2 supports both IMail 6 and IMail 7.1, with IMail 7.1 being the default. Since the interfaces between the two versions have changed, if you would like to use IMail 6, you must set the version option to IMail 6 or EmerAuth may cause IMail 6 to function improperly.

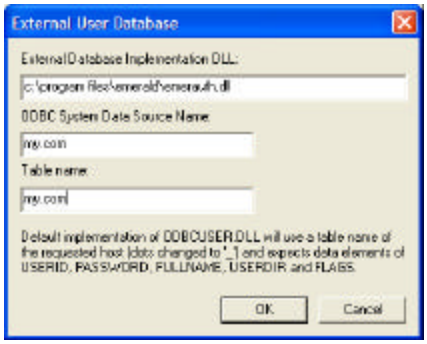
Please Note: EmerAuth 4.5.2 ONLY supports IMail 7.1. Since the interface structure between IMail 7.0 and 7.1 is different, using EmerAuth 4.5.2 with IMail 7.0 will cause IMail 7.0 to not function correctly.

Configuration

To configure IMail to work with EmerAuth, you need to create or change the type of a virtual host to External. You can do this either through the IMail Administrator or the IMail control panel. We will be using the IMail Administrator below.

Please note, you should make sure you have configured EmerAuth to connect to your Emerald database before configuring IMail. Several times in the IMail configuration, it will try to connect to the database. If you have not configured EmerAuth first, the check may hang the IMail administrator.





Open the IMail Administrator, go to the Global tab, and click the virtual host admin button. For initial testing, you should create a test domain. IMail only allows one source for user information per domain. Therefore, you can not have a virtual domain with users from both the local IMail database and the External Database. If you switch the type of a virtual host, you may cause all of the current users to not exist anymore.

When defining the Virtual Host, the FIRST alias defined must be the actual domain that matches the domain from Emerald. If there is no aliases listed, the hostname is used (which probably is not correct). For example, if you are server.my.com, then you should make the first alias "my.com".

For the virtual host, select the "Use External User Database" and click Save, and then click the configure button to the right. For the "External Database Implementation DLL" enter the full path to where the EmerAuth is located. Neither the ODBC DSN nor the Table name is currently used. For testing, just put the matching domain from Emerald in for both the DSN and table name. Finally, click OK. As a side note, if you are configuring a new virtual host, you must save the domain before you can configure it (the OK button on the External Database configuration will be inactive until you click save on the Virtual Host Configuration Screen).

If you added a new virtual host, you may need to click on localhost then hit F5 in order to see the new virtual host listed. Double-check your host properties, including the External User Database configuration to make sure the settings were saved.

If you are using IMail6, then you need to create/update the following Registry entry:

Key: HKEY_LOCAL_MACHINE\Software\IEA\EmerAuth\IMailVer
Type: REG_SZ
Value: "60" for IMail 6, "71" for IMail 7.1

Known Problems and Comments

?? Emerald stores additional IMail attributes in the SubAccountData table. Entries are created on the fly when IMail needs to store additional attributes. Some of these attributes are hidden, while others are shown under the Server custom data section.

?? It seems that IMail is loading/unloading the DLL as requests come in. This could incur extra overhead and performance degradation on heavily used servers and negates the effectiveness of the EmerAuth cache.

?? IMail likes a "root" account for each domain. The requirement of such account is not known.

?? The IMail admin may not list users in your domain. This is typically caused by it trying to enumerate the list of users by only calling GetNextUserEntry without calling GetFirstUserEntry first. Since the handle required in GetNextUserUser is created in GetFirstUserEntry, you will see a set of lines in the EmerAuth log like:

```
Dec 22 00:03:17 2001 DllMain          Thread attach
Dec 22 00:03:17 2001 GetNextUserEntry Entering
Dec 22 00:03:17 2001 GetNextUserEntry Invalid connection handle
Dec 22 00:03:17 2001 GetNextUserEntry Leaving
Dec 22 00:03:17 2001 DllMain          Thread detach
```

?? Allow web access is defaulted for each user.

?? If you want to expose all the hidden data for services, you can run this query. This will expose ALL IMail (ExternalSystemType = -2) fields. You can selectively set the hidden field to 0 for those to show, and 1 for those to hide:

```
Update SubAccountDataTypes Set Hidden = 0 Where ExternalSystemType = -2
```

?? For some reason, the Web messaging does not work right correctly by itself. If you log into the web messaging before using a POP/IMAP client to connect, no folders are accessible (all are listed as Invalid). However, after using something like Netscape or Outlook to connect to the account, all folders show up correctly in web messaging.

?? Users must user their fully qualified user@domain for their username when logging into the Web Messaging services. This is also true for POP and IMAP username configurations.

?? Some Personal preference options may not be saved.

6. Serv-U

Serv-U is a flexible FTP server for the Windows platform, with extensive support for links, multiple users, etc. Please see www.cat-soft.com for information on obtaining Serv-U and a more detailed list of its incredible features.

As of version 2.0c, it supports an External Authentication DLL to allow Serv-U to authenticate and get user information from another database. With EmerAuth, the integration between Emerald and Serv-U allows for seamless management of users. The largest concern of NT based management is how to give users home pages. This solution allows you to give you users home page facility without having to give them an account on an NT machine or use another facility to manage the user security access.

Configuration

Once you install the EmerAuth, you need to modify your serv-u.ini file to configure Serv-U to use it. The main section that needs to be updated is the External section. You can add either the ClientCheckDLLx and EventHookDLLx sections. The second is only needed if you want to gather file transfer information into the database.

```
[EXTERNAL]
ClientCheckDLL1=c:\emerald\EmerAuth.dll
EventHookDLL1=c:\emerald\EmerAuth.dll
```

Please see the Serv-U documentation for more details on the serv-u.ini configuration changes.

How it works

EmerAuth now supports both the Authentication and Event hooks of Serv-U. You can use them independent of each other, but it typically makes more sense to them together, or just the authentication hook.

When Serv-U is started after the above change is made, it will verify and initialize the EmerAuth. This triggers the DLL to connect to the specified ODBC DSN. You MUST have this configured before running Serv-U or the external authentication will always fail.

Authentication

When a user logs in, Serv-U asks the DLL to authenticate the user. The DLL will do a lookup in the SubAccounts table for EITHER a login or shell matching the username, and a password matching the FTP password. If these match, Serv-U will then ask the DLL for the home directory. This is the SubAccounts.HomeDir field for that user.

If the user does NOT exist in Emerald, Serv-U will then search its own local user database. Therefore, you can setup special situations, including anonymous access using the user interface of Serv-U, since it is more feature rich than Emerald for those kind of users.

Event Hooks

The Event hooks allow EmerAuth to store file transfer details in the database for each user. You can then configure Emerald to charge customers based on this information.

When a user completes an upload or download, EmerAuth will add an entry to the FileTransfers table with the user's AccountID, Date, Filename, bytes, and the direction (1=upload, 0=download).

Supported Functions

The user will have full permissions for their directory tree. Serv-U will be in relative path mode, which means the directory you specify is the root directory or top level directory the user can access. Nothing below the user's home directory will be accessible, unless you use the advanced features of Serv-U (links) to make them available.

User quotas are also supported via the HomeDirLimit field in the SubAccounts table. If this field is 0 or NULL, the user will not have a quota. If the field is positive, the user will be limited to that amount of space (in KB) in the directory specified by HomeDir.

Known Problems

Some of the advanced features of Serv-U are not available to customers in the Emerald database. This includes the IP restrictions, ratios, and others.

7. DNews

DNews is a powerful NNTP server. Please see www.netwinsite.com for information on obtaining DNews and a more. As of version 4.6, DNews supports an External Authentication DLL to allow external authentication With EmerAuth, the integration between Emerald and DNews allows easy management of users.

Configuration

Once you install the EmerAuth, you need to modify your dnews.conf file to include the following lines:

```
auth_extern true
auth_lib c:\emerald\emerauth.dll
```

That will tell Dnews to try and authenticate users using the emerauth.dll. You will also need to modify your access.conf file to include entries for the group. A sample might be:

:logoff:::
myisp.com:read,post:::
:read,post:,groups=PPP Filter::,!*sex*

The access.conf file is very tricky to configure right (and remember the last matching rule applies). Please see the DNews documentation for more details on the dnews.conf and access.conf configuration changes.

How it works

When DNews receives a connection from a reader, the reader can supply credentials. If the reader supplies a username/password, then DNews will connect to the EmerAuth to try and verify the user. If the user is verified, the EAS will return the user's AccountType from the SubAccounts table to DNews. DNews will then look for a group with the same name, and grant the user the permissions specified by that group. See the DNews documentation on how to define a group in DNews.

Known Problems

The DNews API is fairly new and may change to add additional functionality. Currently DNews opens the DLL up and closed it for each user request. This can require more over head than usual.

8. Registry Settings

Warning: Changing values in the registry for Windows NT can cause the system to become unstable or stop working. Always use caution when manually changing registry entries.

EAS stores and reads configuration information from the following registry path:

HKEY_LOCAL_MACHINE\Software\IEA\EmerAuth

EmerAuth only reads the registry values at startup. If you change a value, you must re-start the application using EmerAuth for the change to take affect.

Listing

Following is a list of Registry values used by EmerAuth.

Registry	Description
IgnoreCase	Ignore case when comparing username and password. Set to 1 to ignore username case, 2 to ignore password case, or 3 to ignore both.
ODBCDataSource	Specified then ODBC DataSource Name to use for the ODBC connection. This is found under HKEY_LOCAL_MACHINE\Software\IEA\Common.
ODBCUsername	The username for the ODBC connection. This is found under HKEY_LOCAL_MACHINE\Software\IEA\Common.
WCPassword	The password for the ODBC connection. This is found under HKEY_LOCAL_MACHINE\Software\IEA\Common and is encrypted.
Logfile	The logfile used for logging errors and general information to. This should be a fully qualified path, since the current working directory of the DLL will vary depending on the application calling it.
ESID	This is only used with the NTMail API. The ESID should correspond to the ExternalSystemID specified in Emerald. This can be blank or left out if an ExternalSystemID is not used.
MailboxAccountID	If set to 1, EmerAuth will use the AccountID for the user's Mailbox directory name. Any other value (and the default) is to use the user's login name.
Options	If set to 1, EmerAuth will store file transfer information into the File Transfers table.
ODBCMaxConnections	The number of open connections EmerAuth can have to the SQL DB. The higher this number the more concurrent connections EmerAuth can manage. However, raising this number requires that your DB can handle that number of concurrent connections. Be very careful, as raising this number to high can have a negative affect on performance under very heavy loads. The default is 8. This is found under HKEY_LOCAL_MACHINE\Software\Common.
CacheLife	This value tells EmerAuth how long a user entry can stay in memory, before it must refresh the entry from the DB. For heavy servers, raising this number can increase performance (reduce DB load), but at the cost of delayed updates if you change user information in the DB. The value is in seconds, and the default is 1200 (20 minutes).
CompanyName	The name of the Company that the key is Licensed to.
ConfigServerPort	The port number that you want EmerAuth to run on.
Debug_flag	A Numeric value to specify the level of debug.

License	The license key.
ServiceName	The name of the Service that can be installed.
IMail6	If set to 1, EmerAuth will work with IMail 6.0, if set to 0, EmerAuth will work with IMail 7.0. Note: This must be set for the right version otherwise EmerAuth will not work correctly.

9. Supported Database Systems

Although EmerAuth is designed to use ODBC for database connectivity, not all ODBC drivers and SQL statements are the same. EmerAuth will check with the ODBC driver and automatically switch to support the RDBMS, if it has internal knowledge of the RDBMS (see the list below). Otherwise, EmerAuth will default to Microsoft SQL server mode. You can modify the DBM registry entry to force EmerAuth into a particular mode if you are using an unknown database.

Microsoft SQL Server

EmerAuth can be an enterprise-wide solution when used with Microsoft SQL server. The inherent Client/Server design allows multiple clients to be the database simultaneously, without taking a performance hit. SQL Server is also suited to handle tables that can contain over one million records, and includes replication and fail safe operations.

When EmerAuth is used with Microsoft SQL Server, almost all SQL statements are stored procedures. This provides maximum flexibility and control of the database interaction. Below is a list of stored procedures used.

Name	Description
VerifyUser	Check user information for Generic API.
VerifyMailUser	Check user information for Mail API.
VerifyNewsUser	Check user information for News API.
VerifyFTPUser	Check user information for FTP API.

Below is a list of the stored procedures that the EmerAuth will call. The parameters and returned columns must be of the same type, but the stored procedures can be modified to the database design if you are not using Emerald.

```
CREATE PROCEDURE VerifyMailUser @username varchar(32), @domain varchar(32), @esid integer AS
Select Login, Shell, EMail, d.MailDomain, Password, HomeDir
        From MasterAccounts ma, SubAccounts sa, Groups g, Domains d, AccountTypes at
        Where ma.CustomerID = sa.CustomerID
                AND ma.GroupID = g.GroupID
                AND g.DomainID = d.DomainID
                AND at.AccountType = sa.AccountType
                AND at.ExternalSystemID = @esid
                AND ( ((Login=@username OR shell=@username) AND d.Domain=@domain)
                        OR Email = @username + "@" + @domain )

CREATE PROCEDURE VerifyFTPUser @username varchar(32) AS
Select Login, Shell, Password, HomeDir, HomeDirLimit
        From MasterAccounts ma, SubAccounts sa
        Where ma.CustomerID = sa.CustomerID
                AND sa.CustomerID=ma.CustomerID
                AND (Login = @username or Shell = @username or EMail = @username)
                AND sa.Active<>0 AND ma.Active <> 0
                AND DateAdd(Day, ma.Extension+ma.OverDue, maExpireDate) >= GetDate()


CREATE PROCEDURE VerifyNewsUser @username varchar(32) AS
Select Login, Shell, Password, AccountType
```

```
From MasterAccounts ma, SubAccounts sa
Where ma.CustomerID = sa.CustomerID
        AND (Login=@username OR shell=@username OR Email = @username )
        AND sa.Active<>0 AND ma.Active <> 0
        AND DateAdd(Day, ma.Extension+ma.OverDue, maExpireDate) >= GetDate()
```

Microsoft Access

Although Access is not designed to be used in multi-user situations or enterprise wide implementations, it is a very easy to use and powerful database for a single application. There is a significant performance issue when multiple users access the database, though. Since RadiusNT must have the database open at all times, this can become an issue as you grow. There are also no built-in replication or fail safe capabilities either.

EmerAuth will internally create all SQL Statements for MS Access. This limits the flexibility of the database design to follow the Emerald layout, but does not limit the power or features of what EmerAuth can offer.

A fully working Access 7.0 database is included with the RadiusNT distribution. You can use this as a starting point to test or build additional features or options that you would like to use.

Sybase SQL Server

EmerAuth supports operation with Sybase the same as Microsoft's SQL Server. Please see the above Microsoft SQL Server section for an overview. However, the scripts to create the database itself will differ, since there are slight differences between Microsoft's TSQL and Sybase's TSQL. Please see the RadiusNT distribution for an example set of scripts for creating a database under Sybase.

Oracle

EmerAuth supports operation with Oracle in a similar fashion to MS Access. Each SQL query is built into EmerAuth and executed on the fly. This differs from Microsoft and Sybase in that it does not rely on stored procedures or additional database configuration (besides the base tables).

10. Trouble Shooting

Although we have went to great strides to make the installation and use of EmerAuth as easy as possible, problems and errors will sometimes happen. Below are some common problems and solutions to installing and using

Installation and Setup Problems

?? When my application attached to EmerAuth, it returns as error saying the DLL could not be initialized.

When an application attaches to EmerAuth, there are some initial checks EmerAuth must perform. The very first one is to attach to the database, verify connectivity and correct database license. You must have an Emerald or RadiusNT Enterprise license in your database for EmerAuth to function. Otherwise, it will return an error to the calling application and fail. Please contact IEA Software sales if you have a question pertaining to the license.

Operation Problems

?? Can I run multiple instances of the EmerAuth on the same computer?

Yes. The EmerAuth will keep each instance separate and work correctly.

?? Can I run multiple instances of the EmerAuth on different computers all pointing to the same database for load balancing or fail over?

Yes. One of the best features of EmerAuth is the ability to run it on multiple machines. This is an excellent choice for mail servers or ftp servers that can cross mount user information. For example, if you have two licenses for Serv-U, you can run it on two different machines, both supporting the EmerAuth. Since the user home directories are a UNC, either machine can access the home directories and provide correct functionality. NTMail can also be setup in a similar function to have a backup use a primary server's file share.

Please check the licensing of all applications, including the EmerAuth, to make sure you are not violating a license if you are using EmerAuth on more than one machine.