EMGRAFT 2FA & AAA

TWO FACTOR AUTHENTICATION AND AUTHENTICATION, AUTHORIZATION AND ACCOUNTING SOLUTIONS

With maturing mobile technologies, booming global markets and heightened focus on disaster preparedness, remote access control has become a business imperative. The modern mobile workforce demands secure access to more resources from more remote devices and platforms than ever before.

EMGRAFT 2FA has a number of features which are commonly found in RADIUS servers, and additional features which are not found in any other free software server.

AAA, at its core, is all about enabling mobility and dynamic security. Without AAA, a network must be statically configured to control access, IP addresses must be fixed, systems cannot move, and connectivity options should be well defined. Even the earliest days of dialup access broke this static model, thereby requiring AAA. Today, the proliferation of mobile devices, diverse network consumers, and varied network access methods combine to create an environment that places greater demands on AAA.

HIGHLIGHTS

- Complete support for RFC 2865 and RFC 2866 attributes, along with a Vendor-Specific Attributes
- Authorization types are some of the methods which are supported:
  - AD, LDAP, MySQL DB, PostgreSQL DB, Oracle SQL DB, IBM's DB2
- Authentication types are some of the methods which are supported:
  - Clear-text password in local configuration file (PAP)
  - Encrypted password in local configuration file.
  - CHAP, MS-CHAP, MS-CHAPv2.
  - Authentication to a Windows Domain Controller (via ntlm_auth and winbindd).
  - LDAP (PAP only).
  - Kerberos authentication.
  - X9.9 authentication token (e.g. CRYPTOCard).
  - PEAP, EAP-FAST, EAP-TTLS, with embedded authentication methods.

EMGRAFT 2FA & AAA SOLUTIONS

- Emgraft 2FA & AAA facility:
  - Grant access to classified information to true users.
  - User friendly and configurable authentication policies that is compatible to various applications and security needs.
- Define policies for the token management, system configuration, self service, authentication, authorization, enrolment and auditing.
- Define actions of trigger events with reaction such as user email, SMS notification or custom log-messages.
- Perform audit with a secure authentication process that stores log trails of events, token involved, client origin and more detailed information.
- Enable authentication of users from different database
  - SQL databases.
  - OpenLDAP.
  - Active Directory.
  - SCIM servers.
- Authentication mechanism for different types of server:
  - RADIUS (with the Emgraft 2FA & AAA RADIUS plugin)
  - Other plugins available:
    - PAM (supporting Offline OTP).
    - Apache2.
    - Wordpress.
    - And more.
- Two (2) step verification methods using 2-FA and challenge code:
  - PIN code via SMS.
  - PIN code via email.
  - PIN code via Telegram messenger.
  - Soft Token or Push Token.
  - Yubikey.
  - x509 Certificate Token.
  - RADIUS.
  - And more.

ENFORCES PASSWORD POLICIES USING 2-FA

DEFINE POLICIES FOR AUTHNTICATION

ENABLE AUTHENTICA-TION FROM DIFFERENT DATABASE

SECURE "CREDENTIAL STORAGE" FACILITY

AUDIT TRAIL RECORD

EMGRAFT SYSTEMS SDN. BHD. (875234-V)

- Block C2, UPM-MTDC
  Technology Incubation Center 1,
  Lebuh Silikon, Universiti Putra Malaysia,
  43400 Serdang, Selangor, Malaysia.
- +603 8959 1928
- +603 8941 1689
- sales@emgraft.com
- http://www.emgraft.com

MSC MALAYSIA Status Company

Copyright © 2015-2021 Emgraft Systems Sdn Bhd. All rights reserved.