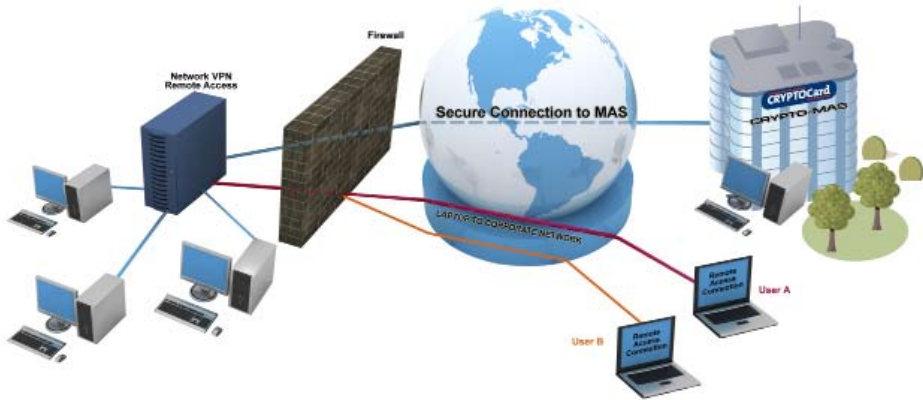


# CRYPTO-MAS

## Groups and Access Control

CRYPTO-MAS delivers hassle free and affordable authentication for users who require access to a network or web site. Many companies now have multiple access points and have implemented comprehensive architectures to group users and adopted sophisticated mechanisms for controlling access for certain groups. CRYPTO-MAS has unique features which complement these mechanisms to ensure that a network or web site is absolutely secure from non-authorized users.



Every user that wants access to a network must first be known to that network. This is done in a number of ways, but in short their details must be known to the access device or web site and they must also be known to the CRYPTO-MAS service. When initially entering the users details into CRYPTO-MAS it is possible to assign them to specific groups.

Putting users into groups within CRYPTO-MAS has a number of benefits:-

- Certain groups can be set-up to access certain applications only
- It is possible to restrict access to certain groups
- It is possible to schedule provisioning of the service to certain groups of users on certain days – aiding better service and support
- CRYPTO-MAS can be used with different token types, so it might be ideal to have groups of users for certain token types – maybe to help support or management reporting
- Groups of users can have different parameters set within CRYPTO-MAS

Using the Group feature for management or support purposes is easy to understand and easy to set-up. Using CRYPTO-MAS to control access using the Group feature – in-conjunction with the access device/application itself - requires a more detailed understanding of how the network and CRYPTO-MAS need to work together.

There are basically two points at which additional access security can be applied to specific Groups of users:-

1. After the authentication process - an access device or application can apply access restrictions following a successful authentication. This scenario is catered for within CRYPTO-MAS with the Radius Return Attributes feature.
2. As part of the authentication process - the Authentication Server will not authenticate a user that is not associated with a valid group or IP address. This scenario is supported by the Access Control list feature within CRYPTO-MAS.

Firstly, lets look at scenario 1, where we use CRYPTO-MAS to work in parallel with RADIUS Return Attributes (RRA). RRA is a feature of the

### CRYPTO-MAS Key Features:

- Incorporates extensive Radius Return Attributes
- Delivers comprehensive access control mechanisms
- Provides flexible deployment capabilities
- Easy to integrate into existing access architecture

## CRYPTO-MAS Groups and Access Control

RADIUS protocol and is increasingly used within sophisticated network access devices, such as Juniper's AS series, in order to provide greater access control. Many companies now use the RRA feature set to apply access restrictions following a successful authentication. In many companies, the attribute commonly used for this process is the Group attribute – which allows for users to be allocated to a specific access groups, such as HR, Finance, Sales etc.

In this scenario, what will happen is that when the user enters their user name and OTP/PIN, CRYPTO-MAS will check that they are valid users and basically send an "OK" to the access device/application. However, rather than the access device simply allowing access, CRYPTO-MAS will also send back a packet of data that tells the device that they are a valid user for a specific Group only – HR for example. If that user is not set up in that group within the RADIUS server, then they will be denied access – as in the above diagram, where User A gets access to the HR system and User B does not.

This whole process allows CRYPTO-MAS to be used in parallel with some of the advanced features that are increasingly common within networks where access needs to be restricted to certain applications – typically HR and finance systems contain the most sensitive data and so restrictions need to be applied.

Setting up CRYPTO-MAS to work in this way is incredibly simple and involves just a couple of clicks during the initial set-up under the Group menu – where a number of options are also provided which allow the service to be compatible with a wide range of specific vendor attributes.

Scenario 2 is typically used to provide similar controls in the event of an access device or application not supporting RADIUS. This is likely to be the case when CRYPTO-MAS is being used to secure a web site or collaboration portal – an increasingly common requirement.

In this scenario, the access restriction requirements are still the same, i.e.; we want to restrict access to the HR system. However, in this case we need to approach this in a slightly different way and

associate users with groups or alternatively base their access permissions on their IP address. We can then set-up CRYPTO-MAS to allow or deny access to certain groups of users.

To do this within the service takes no more than entering data into specific tables within the Group menu option – where we set the Group name and the range of IP addresses that are permitted to access the network.

Both these extremely useful functions provide valuable integration and support benefits to organisations of any size. Further details are explained in CRYPTOCARD's administrative guides.



**CryptoCard Certified Partner**



Tel North: 0151 2031400 Tel South: 0118 9071600  
Email: [Info@castleforce.com](mailto:Info@castleforce.com) Web: [www.castleforce.com](http://www.castleforce.com)

**CRYPTOCARD**  
Secure Your World.