Integrating PAM with TACACS/RSA

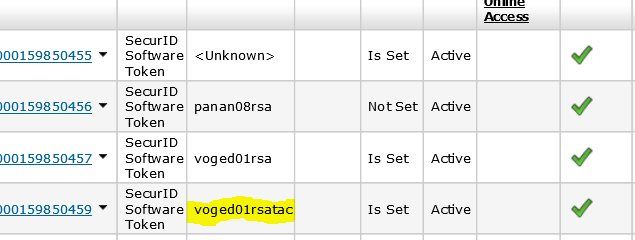
One of the features of Cisco ACS is the configuration of External Identity Stores, one of which is RSA. This document explains how to enable PAM to authenticate through the Cisco ACS to the RSA server. Bear in mind that this is not fully supported yet, as some RSA features are not likely to work through the Cisco ACS. Specifically, the New Pin dialogue and New Token Mode require interaction that may not yet be possible. If the pin is already assigned to the token then this procedure will work fine. If the token becomes out of sync then it will be necessary to put it back into sync outside of PAM.

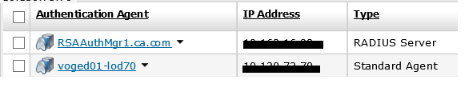
To start with, here are some basics about the RSA configuration. First, here are some tokens. Not the user names configured in the RSA server are associated with the various tokens. Each token will have its own pin and will generate a different token code, possibly of different lengths, at some configured interval. The one with userid voged01rsatac is the one used in this example.

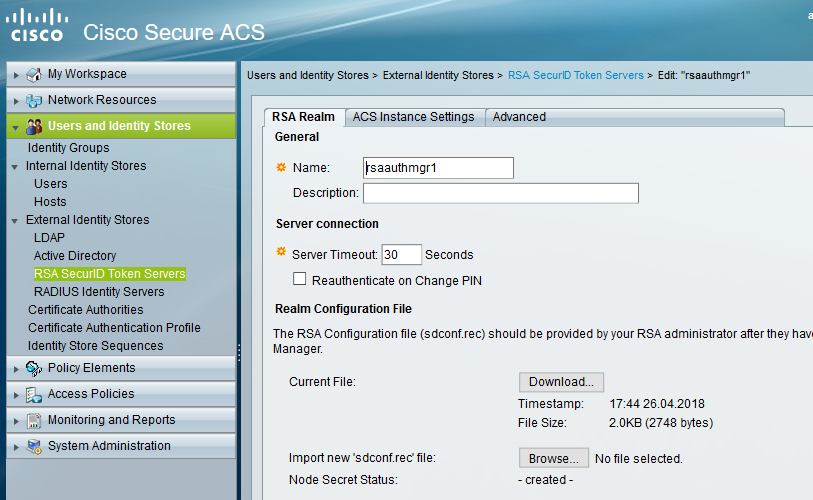
It is also necessary to configure an Authentication Agent entry into the RSA server, in order to allow the Cisco ACS to use the configured token.

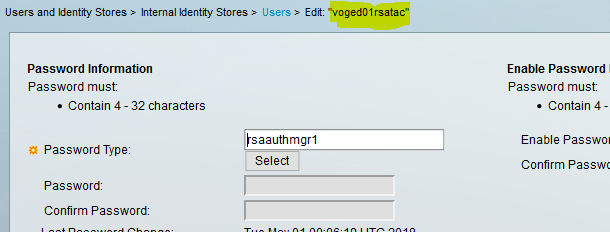
The next step is to configure the Cisco ACS. The first step is to configure RSA as an External Identity store. This includes loading the sdconf.rec provided by the RSA server.

The next step is to configure a user in Cisco ACS to match the user assigned in the token. You don’t configure a password for the user. Instead you point at the External Identity Store configured for RSA.









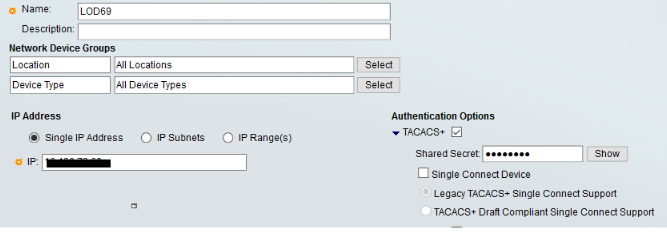
An entry is needed on the Cisco ACS, to allow PAM to authenticate. This will include setting the address and the Shared Secret.

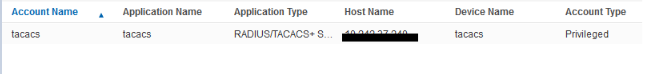
In order to configure TACACS into PAM it is necessary to configure a device for the Cisco ACS. A Target Application and Target Account must then be configured. The Target Account will hold the Shared Secret configured on the Cisco ACS.

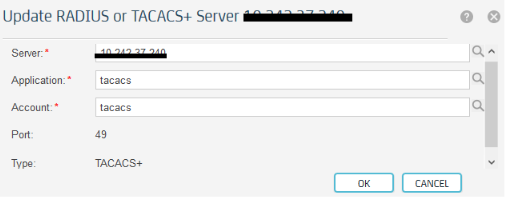
The Target Account is then configured into the 3rd Party page, on an entry for a TACACS server.

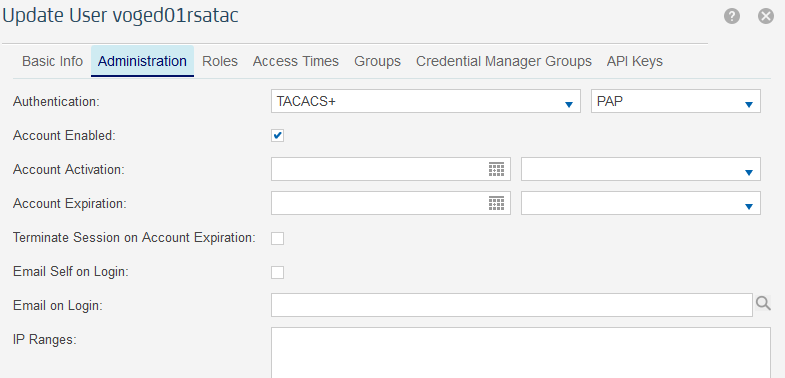
The last step is to configure and account that is set for TACACS Authentication, or configure a group set for TACACS Authentication, with the appropriate users added. The username(s) must match those configured into the Cisco ACS and RSA servers.

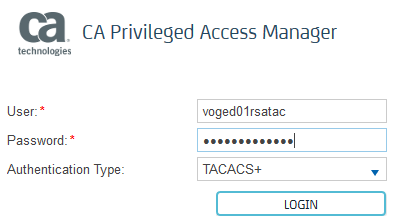
With all this done the user will be able to login to PAM, with TACACS selected, but with RSA Credentials provided. The PIN and Token Code will be entered into the Password field.











This document is intended only as a guide, as each implementation of RSA and Cisco ACS may vary. The steps listed here worked in the Support test environment. Adjustments may be needed to get this working in a specific environment. In addition, and as previously tested, Engineering must do more testing to resolve the issues identified earlier in the document, and any others that are discovered.