Initial R&D Doc

16 September 2022   12:48

1. **Product name**: RSA SECURID Authentication Manager

2. **Website**: [RSA Cybersecurity and Digital Risk Management Solutions](#)
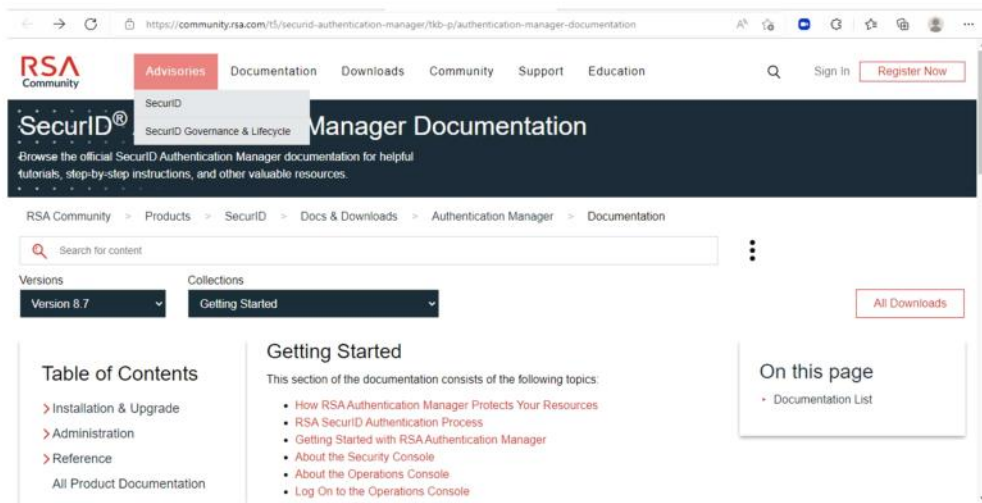
3. **Product Description**:

RSA is Security solution-based firm which has been in the industry for the past 30 years. RSA provides wide range of solution for on premise, cloud, and hybrid Infrastructure.

   1. SecurID
   2. ID Plus

4. **RSA SecurId Products**:

5. SecurID Components

- **Authentication Manager**: This is the Administration module of the system. Here the token generating components are mapped with the identity of the user. This module is also responsible for different actions. It is divided into two parts Security Console and Op's Console. Security Console is responsible for Authentication Request management, System management, Credential management whereas Op's Console s responsible for backup of the system, Replica machine management, patching and update of the system is performed.

- **Agent:** This is the gatekeeper of the resource. There are over 300+ customizable templates offered by RSA. API can also be integrated in this module.

- **Token Generator**: It can be a Legacy USB Token Generator, Software, mail, mobile app, SMS, Phone Call, QR Code etc.
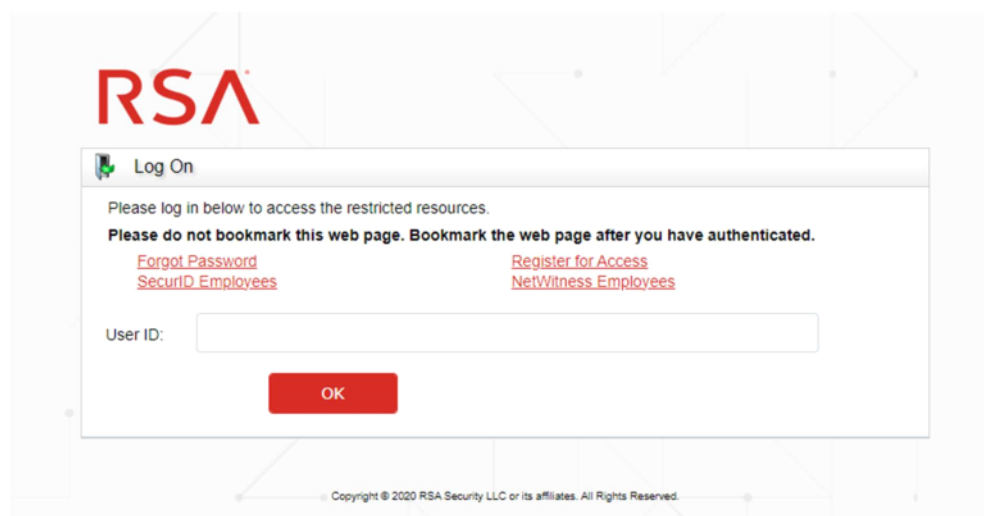
6. Typical Operation Process:

I. User access the Agent and enters his credentials like email and password along with the token that is generated.

II. The data is consumed by the agent then sends them to Authentication Manager for validation if the Credential and the token are valid then the user is granted permission to the resource. If the credentials are invalid then the user cannot access the resource.

III. The whole actions that happened in the session is logged on to the Authentication Manager.

IV. If the User credentials are compromised the user is notified and is prompted for authentication till the problem is resolved thus decreasing the attempts unauthorized login.

V. The Whole validation of the user is done by a sub module of the Administration Manager called CT-KIT.

VI. As mentioned above the token can be generated by a Legacy USB Key fob, Via App, SMS, call, mail, software, or scanning the QR generated by the system.

VII. In all the cases the device or software is mapped to the user initially. All the above modes of token generation has no expiration date except the USB Key Fob. The USB Key Fob has a expiration date after which they will be able to authenticate. In such cases a new USB Key Fob is mapped to the user in the Administration Manager.

Inbuilt SIEM Tools: The RSA has a in built tool called RSA Security analytics which is a combination of the RSA Envision and Net Witness. The Net witness was bought by EMC and was later added to the Envision to make it more efficient.

Trial version: The trial version of the software is not available for public. You need to be registered and Licensed user to download.

After trying with Organization mail it denied access.

Additional resources required:

Log availability:

Reference:

RSA SECURID installation guide:

SecurID Authentication Manager Documentation - RSA Community